On non-square order Tate-Shafarevich groups of non-simple abelian surfaces over the rationals

D I S S E R T A T I O N

zur Erlangung des akademischen Grades

doctor rerum naturalium (Dr. rer. nat.)
im Fach Mathematik

eingereicht an der
Mathematisch-Naturwissenschaftlichen Fakultät II
Humboldt-Universität zu Berlin

von
Dipl.-Math. Stefan Keil

$$\frac{\#Ш(A/K)}{\#Ш(B/K)} = \frac{\#\ker \varphi_K}{\#\operatorname{coker} \varphi_K} \frac{\#\operatorname{coker} \varphi_K^\vee}{\#\ker \varphi_K^\vee} \prod_{v \in M_K} \frac{\#\operatorname{coker} \varphi_v}{\#\ker \varphi_v}$$

Präsident der Humboldt-Universität zu Berlin:
Prof. Dr. Dr. h.c. Christoph Markschies

Dekan der Mathematisch-Naturwissenschaftlichen Fakultät II:
Prof. Dr. Elmar Kulke

Gutachter:
(i) Prof. Dr. Remke Nanne Kloosterman (Humboldt-Universität zu Berlin)
(ii) Prof. Dr. Victor Flynn (University of Oxford)
(iii) Prof. Dr. Tim Dokchitser (University of Bristol)

Tag der Verteidigung: 4. Februar 2014

Summary

The study of rational points on an abelian variety A over a number field K gives rise to its Tate-Shafarevich group $Ш(A/K)$, which plays an important role in understanding the arithmetic of A/K. The Tate-Shafarevich group is conjectured to be finite, and if it is, then for elliptic curves E/K the Cassels-Tate pairing forces the order of $Ш(E/K)$ to be a perfect square. This implication is false for abelian varieties of dimension 2 or higher. It is known, that if A/K is principally polarised and the order of $Ш(A/K)$ is finite, then this order is a square or twice a square. Poonen and Stoll showed that both cases occur. When A/K is not principally polarised, the situation remains unclear. William Stein constructed for all odd primes $p < 25\,000$, $p \neq 37$, an abelian variety $A_p/\mathbb{Q}$ of dimension $p-1$, such that $Ш(A_p/\mathbb{Q})$ has order p times a square. He conjectures that for any given square-free positive integer k there is an abelian variety $A/\mathbb{Q}$, such that $\#Ш(A/\mathbb{Q}) = k \cdot \square$. However, it is an open question what to expect if the dimension of $A/\mathbb{Q}$ is bounded. Restricting to abelian surfaces $B/\mathbb{Q}$, then the results of Poonen, Stoll and Stein imply that there are examples such that $\#Ш(B/\mathbb{Q}) = k \cdot \square$, for $k \in \{1, 2, 3\}$.

In this thesis we focus in depth on abelian surfaces $B/\mathbb{Q}$, such that there are elliptic curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ and an isogeny $\varphi : E_1 \times E_2 \to B$. We want to compute the order of $Ш(B/\mathbb{Q})$ with respect to the order of the Tate-Shafarevich group of $E_1 \times E_2$, which has square order. To achieve this goal, we explore the invariance under isogeny of the Birch and Swinnerton-Dyer conjecture. The main tool used is the Cassels-Tate equation. For each $k \in \{1, 2, 3, 5, 6, 7, 10, 13, 14\}$ we construct a non-simple non-principally polarised abelian surface $B/\mathbb{Q}$ whose Tate-Shafarevich group has order k times a square. All these examples do not assume the finiteness of the Tate-Shafarevich group.

Furthermore, we compute numerically how often the order of $Ш(B/\mathbb{Q})$ equals five times a square, for cyclic isogenies $\varphi : E_1 \times E_2 \to B$ of degree 5. It turns out that this happens to be the case in approx. 50% of the first 20 million examples we have checked.

Finally, we address the question whether there are only finitely many possible square-free k, such that for a non-simple abelian surface $B/\mathbb{Q}$, we have that $\#Ш(B/\mathbb{Q}) = k \cdot \square$. We prove that if there is a cyclic isogeny $\varphi : E_1 \times E_2 \to B$, then $k \in \{1, 2, 3, 5, 6, 7, 10, 13\}$ and no other values can occur. For general isogenies $\varphi : E_1 \times E_2 \to B$, we show that as long as the two elliptic curves belong to a fixed finite set of elliptic curves, then the number of possible k is finite. We end with presenting two hypotheses, whose validity would imply that there are only finitely many k for all non-simple abelian surfaces $B/\mathbb{Q}$, such that $\#Ш(B/\mathbb{Q}) = k \cdot \square$.

In the appendix, we briefly consider abelian surfaces $B/\mathbb{Q}$ being isogenous to Jacobians $\mathcal{J}$ of hyperelliptic curves over $\mathbb{Q}$. The techniques developed in this thesis allow to understand certain cyclic isogenies $\varphi : \mathcal{J} \to B$. For each k in $\{11, 17, 23, 29\}$, we provide an example with $\#Ш(B/\mathbb{Q}) = k \cdot \square$, assuming the finiteness of $Ш(B/\mathbb{Q})$.

Zusammenfassung

Das Studium der rationalen Punkte einer abelschen Varietät A über einem Zahlkörper K führt zu ihrer Tate-Shafarevich Gruppe $Ш(A/K)$, welche eine große Rolle für das Verständnis der Arithmetik von A/K spielt. Es wird vermutet, daß die Tate-Shafarevich Gruppe endlich ist. Bei elliptischen Kurven E/K zwingt in diesem Fall die Cassels-Tate Paarung die Ordnung von $Ш(E/K)$ zu einem Quadrat. Ist A/K prinzipal polarisiert, so ist bewiesen, daß im endlichen Fall die Ordnung von $Ш(A/K)$ ein Quadrat oder zweimal ein Quadrat ist. Poonen und Stoll haben gezeigt, daß beides eintritt. Für nicht-prinzipal polarisierte A/K bleibt die Situation unklar. William Stein hat für jede ungerade Primzahl $p < 25\,000$, $p \neq 37$, eine abelsche Varietät $A_p/\mathbb{Q}$ konstruiert, mit $\#Ш(A_p/\mathbb{Q}) = p \cdot \square$. Er vermutet, daß es für jede quadratfreie positive ganze Zahl k eine abelsche Varietät $A/\mathbb{Q}$ gibt mit $\#Ш(A/\mathbb{Q}) = k \cdot \square$. Jedoch ist es weiterhin ein offenes Problem was zu erwarten ist, wenn die Dimension von $A/\mathbb{Q}$ beschränkt wird. Betrachtet man ausschließlich abelsche Flächen $B/\mathbb{Q}$, so liefern die Resultate von Poonen, Stoll und Stein Beispiele mit $\#Ш(B/\mathbb{Q}) = k \cdot \square$, für $k \in \{1, 2, 3\}$.

Diese Arbeit fokussiert tiefgehend auf nicht-einfache abelsche Flächen $B/\mathbb{Q}$, d.h. es gibt elliptische Kurven $E_1/\mathbb{Q}$ und $E_2/\mathbb{Q}$ und eine Isogenie $\varphi : E_1 \times E_2 \to B$. Relativ zur quadratischen Ordnung der Tate-Shafarevich Gruppe von $E_1 \times E_2$ soll die Ordnung von $Ш(B/\mathbb{Q})$ bestimmt werden. Um dieses Ziel zu erreichen wird die Isogenie-Invarianz der Vermutung von Birch und Swinnerton-Dyer ausgenutzt. Als Hauptwerkzeug dient die Cassels-Tate Gleichung. Für jedes $k \in \{1, 2, 3, 5, 6, 7, 10, 13, 14\}$ wird eine nicht-einfache, nicht-prinzipal polarisierte abelsche Fläche $B/\mathbb{Q}$ konstruiert, mit $\#Ш(B/\mathbb{Q}) = k \cdot \square$. Alle diese Beispiele setzen die Endlichkeit von $Ш(B/\mathbb{Q})$ nicht voraus.

Des weiteren stellt sich mittels computergestützter Berechnungen heraus, daß bei circa 50% der ersten 20 Millionen berechneten zyklischen Isogenien $\varphi : E_1 \times E_2 \to B$ vom Grad 5, die Ordnung von $Ш(B/\mathbb{Q})$ gleich fünf mal ein Quadrat ist.

Abschließend wird auf die Frage eingegangen, ob es nur endlich viele mögliche quadratfreie k gibt, so daß für nicht-einfache abelsche Flächen gilt, daß $\#Ш(B/\mathbb{Q}) = k \cdot \square$. Ist $\varphi : E_1 \times E_2 \to B$ zyklisch, so kann gezeigt werden, daß $k \in \{1, 2, 3, 5, 6, 7, 10, 13\}$ und keine weiteren Werte für k können auftreten. Bei allgemeinen Isogenien $\varphi : E_1 \times E_2 \to B$ gilt, solange E_1 und E_2 aus einer festen endlichen Menge elliptischer Kurven gewählt werden, daß dann die Anzahl der möglichen k endlich ist. Zuletzt werden zwei Hypothesen vorgestellt, die implizieren würden, daß es insgesamt für alle nicht-einfachen abelschen Flächen $B/\mathbb{Q}$ nur endlich viele k gibt, mit $\#Ш(B/\mathbb{Q}) = k \cdot \square$.

Im Anhang wird kurz auf abelsche Flächen eingegangen, welche isogen zu der Jacobischen $\mathcal{J}$ einer hyperelliptischen Kurve über $\mathbb{Q}$ sind. Mit den in dieser Arbeit entwickelten Techniken können, anhand gewisser zyklischer Isogenien $\varphi : \mathcal{J} \to B$, für jedes $k \in \{11, 17, 23, 29\}$ Beispiele mit $\#Ш(B/\mathbb{Q}) = k \cdot \square$ gegeben werden, sofern $\#Ш < \infty$.

Acknowledgements

This thesis would not have been possible without the constant support and encouragement of my advisor Remke N. Kloosterman. I am very thankful for his immense patience, for his availability and insightful feedback, and especially for his enthusiasm for mathematics, which inspired me throughout the last three years. I also want to thank the reviewers for their interest in this work and my mentor Klaus Altmann for giving advice whenever I asked for it.

I am especially grateful to Alex Bartel, Tim and Vladimir Dokchitser, and Matthias Schütt for the many discussions and conversations we had, for their suggestions and explanations, and the time they took to address my problems and satisfy my curiosity. Moreover, I would like to thank Noam D. Elkies, Tom Fisher, and Bjorn Poonen for pointing out particular and relevant details concerning my work. I want to express my special thanks to Samir Siksek and John Cremona for their frequent hospitality at Warwick University. It was a real pleasure to be around at so many conferences and workshops. In the same breath, I like to thank Barinder Banwait for sharing so many nice moments at summer schools and conferences all over the world and for helping me out whenever I was in need.

Further, I would like to thank all my colleagues from the algebraic geometry group, the arithmetic geometry group, the algebraic number theory group, the IRTG Moduli and Automorphic Forms, and everybody from the Berlin Mathematical School, for providing a pleasant academic environment. My special thanks go to Tommaso Benacchio, Giovanni De Gaetano, Frank Gounelas, Miguel Grados, Barbara Jung, Jennifer Rasch, Christian Wald for the enjoyable time we spent both inside and outside of university. My very special thanks go to Jean-Philippe Labbé for his friendship and for his great readiness to help.

I deeply appreciate the constant love and support of my family. Above all, I am grateful to my parents, whose trust and believe in what I do have given me the confidence and strength to pursue my goals. I want to thank my brothers Sebastian and Timo for being my companions throughout my life, and I am deeply thankful to my grandmother for being so proud of all her grand- and great-grandchildren. I would like to thank my godchild Vivian Kramhöft for her smile and for questioning the world.

I heartily thank my friends Markus Koch, Hanna Sartorius, Jan Meyer, Ellie Gregory, Ariel Garcia, and Rosalía Schultze-Kraft for being my home and family in Berlin. My special thanks go to Juliane Drückler for steadying and encouraging me during the final stretch of writing this thesis. I would also like to thank Marco Köhnen, Nicko C.-W. Horst, Jasmin Schulze, Mareike Eymer, Stefanie John, Dominik Lubian , Jost Wessels and Laura Bingemer for their friendship and unforgettable moments spent together.

I am thankful to the following mathematicians for sharing their knowledge and passion with me on mathoverflow: Michael Albanese, Kestutis Cesnavicius, Pete L. Clark, Brian Conrad, Chandan Singh Dalawat, Vesselin Dimitrov, Olivier Fouquet, Edray Herber Goins, Timo Keller, Cam McLeman, Marc Palm, René Pannekoek, Joseph H. Silverman, Dror Speiser, Michael Stoll, Stefano Vigni, Felipe Voloch, Michael Zieve, David Zureick-Brown, and especially François Brunault, Maarten Derickx, Jordan S. Ellenberg, Henri Johnston, Daniel Loughran, Alexander Stasinski, Christian Wuthrich, and Yuri Zarhin.

I would like to acknowledge the help of the BMS One-Stop Office, with special thanks to Nadja Wiesniewski, Tanja Fagel, and Dominique Schneider. I want to thank Leibniz Universität Hannover for offering me a teaching position at the very beginning and during the final stage of my PhD research. Finally, I thank the Humboldt-Universität zu Berlin for providing an excellent working environment, and the Berlin Mathematical School for their financial support during my studies.

— Berlin, 29$^{\text{th}}$ of November, 2013.

Contents

Summary iii

Zusammenfassung v

Acknowledgements vii

Notation xi

1. Introduction 1
1.1. From diophantine equations to Tate-Shafarevich groups 1
1.2. Work of Cassels and Tate and first examples of non-square order Ш . . . 3

2. Controlling the order of Tate-Shafarevich groups modulo squares 7
2.1. An equation of Cassels and Tate 7
2.2. Isogenies between abelian varieties over local fields 9
2.3. Isogenies of prime degree between elliptic curves over local fields 18
2.4. Non-simple abelian varieties and isogenies with diagonal kernel 22

3. Constructing abelian surfaces $B/\mathbb{Q}$ with non-square order $Ш(B/\mathbb{Q})$ 31
3.1. The local quotient 32
3.2. The global quotient 34
3.3. $N = 5$ and $N = 7$ ($k = 5, 7$) 36
3.4. $N = 6$ and $N = 10$ ($k = 1, 2, 3, 6, 10$) 46

4. Density questions about non-square order Ш and numerical results 55
4.1. Algorithm 55
4.2. Results 60

5. Obstructions to non-square order Ш of non-simple abelian surfaces over $\mathbb{Q}$ 67
5.1. Qudratic twists and cyclic isogenies of elliptic curves over $\mathbb{Q}$ 68
5.2. Cyclic isogenies $\Theta : E_1 \times E_2 \to B_\Theta$ with diagonal kernel, ($k = 13$) 76
5.3. Diagonal multiplication-by-n maps $\Xi : E_1 \times E_2 \to B_\Xi$, ($k = 14$) 81

A. Appendix. A brief glimpse at simple abelian surfaces, $(k = 11, 17, 23, 29)$ 91

Bibliography 95

Notation

Throughout the text, let A/K be an abelian variety A over a field K, i.e. a proper group scheme of positive dimension which is geometrically integral and of finite type over Spec K. Usually, K is a number field, i.e. $K/\mathbb{Q}$ is a finite field extension, or a (p-adic) local field, i.e. $K/\mathbb{Q}_p$ is a finite field extension, or a finite field. Since all fields considered are perfect we do not pay attention to separability, and with $\overline{K}$ we denote a once and for all fixed algebraic closure of K. For a field L containing K, the group of L-rational points is denoted by $A(L)$, with $\mathcal{O} \in A(L)$ being the identity element of the group law. The dual abelian variety of A/K is denoted by $A^\vee := \mathrm{Pic}^0_{A/K}$, and a polarisation of A/K is a symmetric isogeny $\lambda : A \to A^\vee$, such that over $\overline{K}$ we have $\lambda = \lambda_{\mathcal{L}}$, for an ample line bundle $\mathcal{L}$ on $A/\overline{K}$. If $\varphi : A \to B$ is an isogeny between abelian varieties over a field K, then for a field extension L/K we say that φ has a *L-kernel*, if all points in $A(\overline{K})[\varphi]$ are already defined over L, i.e. $A(\overline{K})[\varphi] = A(L)[\varphi]$. If we do not specify the field of definition of an isogeny φ between two abelian varieties which are defined over a field K, then we want φ to be also defined over K.

If K is a number field, then with v we denote a place of K, i.e. an equivalence class of valuations of K, and with M_K the set of all places of K. We have the subset M_K^0 of all finite places (or primes) of K and the subset M_K^∞ of all infinite places of K. With K_v we denote the completion of K at v, and with k_v its residue field, i.e., the quotient of the valuation ring $\mathcal{O}_v$ of K_v by its maximal ideal $\mathfrak{m}_v = \pi_v \mathcal{O}_v$, for a uniformiser π_v. We normalise the absolute value $|\cdot|_v$ on K_v so that $|\pi_v|_v = (\#k_v)^{-1}$. If $v \in M_K^0$ is a place lying over $p \in M_{\mathbb{Q}}^0$, we denote this by $v|p$ and call K_v a p-adic field. In this case $K_v/\mathbb{Q}_p$ is a finite field extension of degree at most $[K : \mathbb{Q}]$. Denote by K_v^{nr} the maximal unramified extension of K_v; thus K_v^{nr} is obtained by adjoining to K_v all n-th roots of unity, for n coprime to the characteristic p of k_v. The absolute Galois group of a field K is denoted by Gal_K. For Galois cohomology we use the usual abbreviation $H^i(K, M) := H^i(\mathrm{Gal}_K, M)$. The *Tate-Shafarevich group* of A/K is defined as

$$Ш(A/K) := \ker\left(H^1\left(K, A(\overline{K})\right) \longrightarrow \prod_{v \in M_K} H^1\left(K_v, A(\overline{K}_v)\right)\right).$$

With ℓ we denote a prime number and by $\mathbb{Z}/\ell\mathbb{Z}$ we either mean a cyclic group of order ℓ or a cyclic Galois module of order ℓ with trivial Galois action. By $\boldsymbol{\mu}_\ell$ we denote the ℓ-th roots of unity as a group scheme or as a subset of $\overline{K}^*$ considered as a K-Galois module. We write $\xi = \xi_\ell \in \overline{K}^*$ for a primitive ℓ-th root of unity. The trivial group is denoted by 0, and by $\square$ we denote a square natural number. We often refer to computations carried out with the software packages Sage [S$^+$13] and Magma [BCP97].

Chapter 1. Introduction

The first part of this introduction is aimed at non-experts. It lays out the historical background of this thesis and motivates the study of Tate-Shafarevich groups through one of the main driving forces of number theory: the classification of rational solutions of diophantine equations. The second part summarises recent developments concerning non-square order Tate-Shafarevich groups and presents the outline of this work.

1.1. From diophantine equations to Tate-Shafarevich groups – history and motivation

One of the classical questions of number theory is to find the integer or rational solutions of *diophantine equations*, i.e. polynomial equations in multiple variables with integer or rational coefficients. For example, it is proven that the equation

$$Y^2 + XY + Y = X^3 + X^2 + 35X - 28$$

has exactly seven solutions (x, y), such that x and y are both rational numbers. These solutions are $(2, 6), (2, -9), (7, 21), (7, -29), (32, 171), (32, -204)$ and $(3/4, -7/8)$.

In general, the question is threefold. Firstly, whether there is a rational solution at all. Secondly, whether there are finitely or infinitely many rational solutions. And thirdly, to list all of them in the finite case, or in the infinite case to describe an algorithm that would eventually produce any given rational solution. All these questions are highly non-trivial problems. Given an arbitrary diophantine equation with integer coefficients, there is no algorithm that can decide whether this equation has an integer solution. This answers Hilbert's tenth problem from 1900 in the negative. It is still unknown if such an algorithm exists for rational solutions. However, for particular classes of diophantine equations there are algorithms that can decide whether there are finitely or infinitely many rational solutions and sometimes whether there is a solution at all.

The case of diophantine equations with only one variable and the cases of linear or quadratic diophantine equations in two variables were established by the number theorists of the 18^{th}-20^{th} century and are essentially contained in Gauß' and Hensel's

Lemma and the Hasse-Minkowski theorem. In case of one variable, there are only finitely many rational solutions and they can be found easily. For diophantine equations of degree one or two in two variables, there is an algorithm which can decide whether there is a rational solution. If the set of rational solutions is non-empty, then it is infinite, and given any rational solution there is an algorithm to compute all other rational solutions. One of the biggest results at the end of the 20^{th} century is Faltings' theorem, formerly known as the Mordell conjecture. It implies that if the projective closure of a diophantine equations in two variables of degree 4 or higher is smooth, then it only has finitely many rational solutions.

It remains to consider cubic equations in two variables. If the projective closure is smooth and contains at least one rational point, such as in the example above, then it is called an *elliptic curve* (over $\mathbb{Q}$). The set of rational solutions of an elliptic curve E is denoted by $E(\mathbb{Q})$ and it is known that $E(\mathbb{Q})$ comes with an additional structure: It forms an abelian group, and thus we can *add* points. For instance, in the above example we have $(3/4, -7/8) + (2, -9) = (32, 171)$ and $(2, -9) + (2, -9) = (7, 21)$. Moreover, it has been conjectured in 1901 by Poincaré and been proven in the 1920s by Mordell, that $E(\mathbb{Q})$ is a finitely generated abelian group, hence

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}\,.$$

It follows that $E(\mathbb{Q})_{\text{tors}}$ is a finite abelian group, called the *torsion* part, and r is a non-negative integer, called the *Mordell-Weil rank* or *arithmetic rank*, or just the *rank* of E. Even after more than 100 years, the study of $E(\mathbb{Q})$ is still a highly active research area. One of the most discussed questions in arithmetic geometry is whether the rank r can become arbitrarily large if one ranges over all elliptic curves over $\mathbb{Q}$. Given an arbitrary elliptic curve it is still a difficult task to compute its rank r. The problem is twofold. From a theoretical point of view, the algorithm which is used to compute the rank of a given elliptic curve is not proven to terminate. Even though one expects the algorithm to eventually terminate in all cases, it has a very long running time when the coefficients of the elliptic curve are sufficiently large. Hence, from a practical point of view, only for elliptic curves with small coefficients one can effectively compute their ranks. The reason that the algorithm is not known to terminate is due to the fact that it only computes an upper bound of the rank. Often, this upper bound equals the rank but the problem is how to detect this. The difference of this upper bound to the actual rank is measured by the so called *Tate-Shafarevich group* Ш of the elliptic curve E, which became a very popular research topic in the beginning of the 1960s.

The Tate-Shafarevich group is a very complicated object, even though it turns out that it is often the trivial group. From its definition one easily derives that it is an abelian torsion group. In 1962, Cassels showed the existence of a very interesting pairing on the Tate-Shafarevich group which implies a surprising fact. If the Tate-Shafarevich group of an elliptic curve is a finite group, then its cardinality is a perfect square. Not much else is known about the Tate-Shafarevich group, but it comes with two very important conjectures, which were also stated in the 1960s. The first one says that the size of the Tate-Shafarevich group is always finite. Besides implying that the Tate-Shafarevich

group is of square order, the validity of this conjecture would imply that the algorithm to determine the rank of E always terminates. Usually, for elliptic curves of rank equal to 0 or 1 one can actually calculate its rank and prove that its Tate-Shafarevich group is finite. This is the result obtained in the mid 1980s until the mid 1990s through the culminated work of Gross, Zagier, Kolyvagin, Wiles and others.

Elliptic curves are 1-dimensional objects and their higher dimensional generalisations are called abelian varieties. In higher dimensions many properties of elliptic curves are still valid, but there are also new phenomena. In 1963, Tate generalised Cassels' pairing on the Tate-Shafarevich group. On arbitrary abelian varieties it does not imply anymore that the order of its Tate-Shafarevich group is a square, provided the order is finite. So one might wonder, whether there are actually non-square order Tate-Shafarevich groups. The answer is indeed yes, but was completely surprising to many people. Probably the reason for this unexpectedness is the fact, that Tate deduced the squareness of the order of Tate-Shafarevich groups of general abelian varieties assuming additional conditions. And then these further assumptions got forgotten and sometimes they were even skipped and Tate was cited wrongly; see [Ste03] for some historical remarks. In 1996, more than 30 years later, Michael Stoll constructed the first example of an abelian variety having non-square order Tate-Shafarevich group, and this started a whole industry to investigate this phenomenon.

The second conjecture concerning the Tate-Shafarevich group is the *Birch and Swinnerton-Dyer* conjecture. It describes a fascinating relationship between all the arithmetic and analytic invariants associated to an abelian variety, including the conjectural existing order of its Tate-Shafarevich group. It is known from the work of Cassels and Tate, that if two abelian varieties are isogenous, i.e. there is a morphism between the two abelian varieties which deforms them into each other, then the Birch and Swinnerton-Dyer conjecture is either true for both of them or false for both of them. Further, this invariance under isogeny of the Birch and Swinnerton-Dyer conjecture establishes a relation between the order of the Tate-Shafarevich groups of two isogenous abelian varieties. This thesis offers an exploration of this relation and it is our main tool to construct abelian surfaces, i.e. two-dimensional abelian varieties, having Tate-Shafarevich groups of non-square order.

Even though we could come up with partial answers to enlighten the phenomena of non-square order Tate-Shafarevich groups, it still bears many of its secrets and studying the Tate-Shafarevich groups of elliptic curves and abelian varieties stays one of the most challenging and fascinating topics of arithmetic geometry and number theory.

1.2. Work of Cassels and Tate and first examples of non-square order Tate-Shafarevich groups – outline of this thesis

Let A/K be an abelian variety over a number field K. Consider its Tate-Shafarevich group $Ш(A/K)$ and denote by $A^\vee$ the dual abelian variety. The Tate-Shafarevich group

comes with a bilinear pairing, called the Cassels-Tate pairing [Cas62], [Tat63]

$$\langle \cdot, \cdot \rangle : Ш(A/K) \times Ш(A^\vee/K) \to \mathbb{Q}/\mathbb{Z},$$

which is non-degenerate in case $Ш(A/K)$ is finite. If A is an elliptic curve E, then the pairing forces the order of $Ш(E/K)$ to be a perfect square, if it is finite. But in higher dimensions, even for principally polarised abelian varieties, this is no longer true in general. Together with a result of Flach [Fla90], the Cassels-Tate pairing gives a strong restriction on the non-square part of the order of $Ш(A/K)$, see [Ste04, Theorem 1.2].

Theorem 1.2.1 (Tate, Flach)**.** *Assume $Ш(A/K)$ is finite. If an odd prime p divides the non-square part of the order of $Ш(A/K)$, then p divides the degree of every polarisation of A/K.*

Corollary 1.2.2 (Poonen, Stoll)**.** *If A/K is a principally polarised abelian variety, then*

$$\#Ш(A/K) = \square \text{ or } 2 \cdot \square.$$

In 1996, Michael Stoll constructed the first example of a principally polarised abelian variety A/K having $\#Ш(A/K) = 2 \cdot \square$. Together with Bjorn Poonen, Stoll [PS99] associated to each principal polarisation λ of A/K a canonical element $c \in Ш(A/K)[2]$, assuming the finiteness of $Ш(A/K)$. They showed that the order of $Ш(A/K)$ is a square if and only if $\langle c, \lambda(c) \rangle = 0$. This is clearly the case if $c = 0$. They showed that $c = 0$ is equivalent to the induced pairing on $Ш(A/K)$ being alternating and also equivalent to the polarisation λ arising from a K-rational divisor. It was already known by Tate [Tat63] that the order of Ш is a square, if such a K-rational divisor exists, as it is the case for elliptic curves E/K. Hence, the induced pairing on $Ш(E/K)$ is alternating, as was shown by Cassels [Cas62] the year before. In case that $c \neq 0$, then the induced pairing is only anti-symmetric, due to Flach [Fla90]. This is the reason why we cannot conclude in general that the 2-primary part of $Ш(A/K)$ has square cardinality.

Stoll's first example of an abelian variety having non-square order Tate-Shafarevich group is the Jacobian of a genus 2 curve over $\mathbb{Q}$, hence it is a principally polarised abelian surface over $\mathbb{Q}$. Thereafter, for every odd prime $p < 25\,000$, $p \neq 37$, William Stein [Ste04] constructed an abelian variety $A_p/\mathbb{Q}$ of dimension $p - 1$, such that $\#Ш(A_p/\mathbb{Q}) = p \cdot \square$. This result led Stein to make the following conjecture.

Conjecture 1.2.3 (William Stein)**.** *As one ranges over all abelian varieties $A/\mathbb{Q}$, every square-free natural number appears as the non-square part of the order of some $Ш(A/\mathbb{Q})$.*

The following question is natural.

Question 1.2.4. *What are the possible non-square parts of the orders of finite Tate-Shafarevich groups for abelian varieties of fixed dimension over a fixed number field? Is this a finite list?*

The motivation of this thesis is to answer Question 1.2.4 in the first possible setting: the dimension of the abelian varieties equals 2 and the ground field is $\mathbb{Q}$. So far, the only known square-free positive integers k which occur as the non-square part of the order of a Tate-Shafarevich group of an abelian surface $B/\mathbb{Q}$ are 1, 2, and 3. We extend this list by providing explicit examples. In short, we prove the following theorem.

Theorem 1.2.5. *For each $k \in \{1,2,3,5,6,7,10,13,14\}$ there exists a non-simple non-principally polarised abelian surface $B/\mathbb{Q}$ such that $\#Ш(B/\mathbb{Q}) = k \cdot \square$. Further, for each $k \in \{11,17,23,29\}$ there exists an absolutely simple non-principally polarised abelian surface $B/\mathbb{Q}$ such that $\#Ш(B/\mathbb{Q}) = k \cdot \square$, provided the Tate-Shafarevich group is finite.*

We briefly sketch the methods applied in this thesis and give an outline of the content. The strategy used to construct abelian surfaces $B/\mathbb{Q}$ having Tate-Shafarevich group of non-square order is based on the invariance under isogeny of the Birch and Swinnerton-Dyer conjecture. The main purpose of this strategy is to circumvent the highly non-trivial problem of precisely determining the order of Tate-Shafarevich groups of abelian varieties. If $\varphi : A \to B$ is an isogeny between abelian varieties over a number field K, then the *Cassels-Tate equation*, which is part of the proof of the invariance under isogeny of the Birch and Swinnerton-Dyer conjecture, gives a formula to compute the quotient of the order of $Ш(A/K)$ divided by the order of $Ш(B/K)$. Thus, if one knows the order of $Ш(A/K)$ up to squares, then one can deduce the order of $Ш(B/K)$ up to squares. Further, φ naturally induces a group homomorphism between $Ш(A/K)$ and $Ш(B/K)$, which is an isomorphism between ℓ-primary parts for primes ℓ not dividing the degree of φ. In particular this means, that if $Ш(A/K)$ is of square order, then a necessary condition for a prime ℓ to divide the non-square part of the order of $Ш(B/K)$ is that ℓ divides the degree of φ.

We focus on $A := E_1 \times E_2$ being a product of two elliptic curves over $\mathbb{Q}$. Hence, $A/\mathbb{Q}$ has square order Tate-Shafarevich group and therefore the non-square part of the right hand side of the Cassels-Tate equation is equal to the non-square part of the order of the Tate-Shafarevich group of $B/\mathbb{Q}$. Further, $A/\mathbb{Q}$ can be described easily by two Weierstraß equations, one for each elliptic curve. An additional advantage of this choice of A is that the possible isogenies $\varphi : E_1 \times E_2 \to B$ are completely classified, as the classification of isogenies of elliptic curves over $\mathbb{Q}$ was accomplished by Mazur, Kenku and others in the early 1980s. It is worth noting, that the construction we use is different from the construction used by Poonen and Stoll, and by Stein.

In Chapter 2 of this thesis, we introduce the *Cassels-Tate equation*. It determines the order of $Ш(A/K)$ relatively to the order of $Ш(B/K)$ in terms of the number of local and global points in the kernel and cokernel of $\varphi : A \to B$, and the number of global points in the kernel and cokernel of $\varphi^\vee : B^\vee \to A^\vee$. Usually the kernels are understood through the definition of φ, and hence we have to determine the structure of local and global points of the cokernels. In the remaining of the second chapter we study the local points of $\operatorname{coker}\varphi$, for general abelian varieties A and B and for the special case of A and B being elliptic curves. This investigation is done by using Galois cohomology. The main tool to understand the local points of $\operatorname{coker}\varphi$ is by studying criteria whether it is maximally unramified. In the last section of the second chapter, we introduce isogenies $\varphi : E_1 \times E_2 \to B$ with diagonal kernel and study their properties. Throughout this thesis, we are mainly interested in such kind of isogenies.

In Chapter 3, we study in detail the situation of cyclic isogenies $\varphi : E_1 \times E_2 \to B$ with diagonal kernel, which are constructed by using elliptic curves over $\mathbb{Q}$ possessing a $\mathbb{Q}$-rational N-torsion point. We are especially interested in the prime cases $N = 5$

and $N = 7$. For all N, those families of elliptic curves can be parametrised by a rational number, and we explain how to express the local quotient with respect to that rational numbers. Further, we give an algorithm with which one can compute the global quotient, provided one knows generators of the Mordell-Weil groups $E_1(\mathbb{Q})$ and $E_2(\mathbb{Q})$. This enable us to produce explicit unconditional examples of non-simple abelian surface $B/\mathbb{Q}$ with non-square order Tate-Shafarevich groups, and thus we partly prove the above theorem.

In Chapter 4, we do extensive numerical calculations for the family of elliptic curves introduced in the last chapter with respect to $N = 5$. We explain how to transform the techniques from the last two chapters into an algorithm using computer software. It turns out that among the first 20 million abelian surfaces in our given family almost 50% of them have non-square order Tate-Shafarevich group, provided the groups are finite. We give heuristic arguments why we expect that a density of 50% of these abelian surfaces should have a Tate-Shafarevich group of non-square order.

In Chapter 5, we study arbitrary isogenies $\varphi : E_1 \times E_2 \to B$ over $\mathbb{Q}$. Using Mazur's (and others) classification of cyclic isogenies of elliptic curves over $\mathbb{Q}$, we can completely determine the possible non-square parts of the order of Tate-Shafarevich groups of $B/\mathbb{Q}$, provided φ is a cyclic isogeny. It remains open whether there are only finitely many possibilities for the non-square part of the order of Tate-Shafarevich groups of arbitrary non-simple abelian surfaces $B/\mathbb{Q}$. We can give an affirmative answer to this question in case the two elliptic curves can only vary in a fixed finite set of elliptic curves over $\mathbb{Q}$. We present two hypotheses, whose validity would imply that the number of possible non-square parts of the order of Tate-Shafarevich groups of arbitrary non-simple abelian surfaces $B/\mathbb{Q}$ is indeed finite. We end this chapter with constructing a non-simple abelian surface $B/\mathbb{Q}$ having Tate-Shafarevich group of order 14 times a square, which is not possible if φ was cyclic. This finishes the proof for the first part of the above theorem.

In Appendix A, we replace the product $E_1 \times E_2$ with the Jacobian $\mathcal{J}$ of a hyperelliptic curve of genus 2 over $\mathbb{Q}$, such that $\mathcal{J}$ possesses a $\mathbb{Q}$-rational torsion point. In the literature, there are known examples of such Jacobians possessing a $\mathbb{Q}$-rational torsion point of square-free order $N = 11, 17, 23, 29$, among other values. Our techniques established in the rest of the thesis are general enough to be able to compute the Cassels-Tate equation for the cyclic isogeny $\varphi : \mathcal{J} \to B$, whose kernel is generated by that N-torsion point. This method leads to the second group of examples that occur in the above theorem and completes its proof.

2 Chapter 2. Controlling the order of Tate-Shafarevich groups modulo squares

In the first section of this chapter, we present the Cassels-Tate equation (2.1). It is associated to an isogeny $\varphi : A \to B$ between abelian varieties over a number field and consists of a local and a global part, which are called the *local quotient* and the *global quotient*. We spend the following two sections computing the local quotient. To understand the cokernels occurring in the local quotient we use Galois cohomology. Our goal is to develop criteria to detect whether the cokernels are trivial, maximal, or maximally unramified. The principal task of the second section is to give criteria for maximal unramifiedness, in case of arbitrary isogenies $\varphi : A \to B$. Our main criterion is Theorem 2.2.19, which is based on a result of Schaefer and Stoll. In the third section, we focus on isogenies between elliptic curves. In the last section, we introduce isogenies $\varphi : E_1 \times E_2 \to B$ having diagonal kernel. Such isogenies give naturally rise to isogenies $\eta_1 : E_1 \to E_1'$ and $\eta_2 : E_2 \to E_2'$. We present our Key Lemma 2.4.5 to control the local quotient. With the Key Lemma it is possible to deduce whether $\operatorname{coker}\varphi$ is trivial, maximal or maximally unramified, provided one knows these properties for η_1 and η_2.

2.1. An equation of Cassels and Tate

In the mid 1960s, Cassels [Cas65] (the elliptic curve case) and Tate [Tat95] (the general case) proved the following theorem to show the invariance of the Birch and Swinnerton-Dyer conjecture under isogeny. Denote by R_A the regulator and by P_A the period of an abelian variety A/K over a number field K. By $c_{A,v}$ we denote the local Tamagawa number of A at a finite place $v \in M_K^0$.

Theorem 2.1.1 (Cassels, Tate)**.** *Let $\varphi : A \to B$ be an isogeny between two abelian varieties A and B over a number field K. Assume that at least one of $Ш(A/K)$ or $Ш(B/K)$ is finite. Then $Ш(A/K)$ and $Ш(B/K)$ are both finite, and*

$$\frac{\#Ш(A/K)}{\#Ш(B/K)} = \frac{R_B}{R_A} \cdot \frac{\#A(K)_{\text{tors}}\,\#A^\vee(K)_{\text{tors}}}{\#B(K)_{\text{tors}}\,\#B^\vee(K)_{\text{tors}}} \cdot \frac{P_B}{P_A} \cdot \prod_{v \in M_K^0} \frac{c_{B,v}}{c_{A,v}}.$$

The product over the Tamagawa numbers is actually finite, since $c_{A,v} = 1$ if v is a place of good reduction. Define $A(K)_{\text{free}}$ to be the quotient group $A(K)/A(K)_{\text{tors}}$ and consider the following induced group homomorphisms.

$$\varphi_K : A(K) \to B(K),\ \varphi_K^\vee : B^\vee(K) \to A^\vee(K),\ \varphi_v : A(K_v) \to B(K_v),$$

$$\varphi_{K,\text{tors}} : A(K)_{\text{tors}} \to B(K)_{\text{tors}},\ \ \varphi_{K,\text{tors}}^\vee : B^\vee(K)_{\text{tors}} \to A^\vee(K)_{\text{tors}},$$
$$\varphi_{K,\text{free}} : A(K)_{\text{free}} \to B(K)_{\text{free}},\ \ \varphi_{K,\text{free}}^\vee : B^\vee(K)_{\text{free}} \to A^\vee(K)_{\text{free}}.$$

We may now reformulate the above quotients in terms of these induced group homomorphisms. This reformulation, which is part of the proof of the above theorem, turns out to be easier to handle for computational purposes, and we use the Cassels-Tate equation only in this description. There are two trivial equalities, namely

$$\frac{\#A(K)_{\text{tors}}}{\#B(K)_{\text{tors}}} = \frac{\#\ker \varphi_K}{\#\operatorname{coker} \varphi_{K,\text{tors}}} \text{ and } \frac{\#A^\vee(K)_{\text{tors}}}{\#B^\vee(K)_{\text{tors}}} = \frac{\#\operatorname{coker} \varphi_{K,\text{tors}}^\vee}{\#\ker \varphi_K^\vee},$$

and two more interesting ones, see the proof of [Mil06, Theorem I.7.3];

$$\frac{R_B}{R_A} = \frac{\#\operatorname{coker} \varphi_{K,\text{free}}^\vee}{\#\operatorname{coker} \varphi_{K,\text{free}}} \text{ and } \frac{P_B}{P_A} \cdot \prod_{v \in M_K^0} \frac{c_{B,v}}{c_{A,v}} = \prod_{v \in M_K} \frac{\#\operatorname{coker} \varphi_v}{\#\ker \varphi_v}.$$

Hence the Cassels-Tate equation becomes

$$\frac{\#Ш(A/K)}{\#Ш(B/K)} = \frac{\#\ker \varphi_K}{\#\operatorname{coker} \varphi_K} \frac{\#\operatorname{coker} \varphi_K^\vee}{\#\ker \varphi_K^\vee} \prod_{v \in M_K} \frac{\#\operatorname{coker} \varphi_v}{\#\ker \varphi_v}. \tag{2.1}$$

In particular,

$$\frac{R_B}{R_A} \cdot \frac{\#A(K)_{\text{tors}} \#A^\vee(K)_{\text{tors}}}{\#B(K)_{\text{tors}} \#B^\vee(K)_{\text{tors}}} = \frac{\#\ker \varphi_K}{\#\operatorname{coker} \varphi_K} \frac{\#\operatorname{coker} \varphi_K^\vee}{\#\ker \varphi_K^\vee},$$

and we call the right-hand side of this equation the *global quotient*. The global quotient clearly breaks into the *regulator quotient* and the *torsion quotient*. The product

$$\prod_{v \in M_K} \frac{\#\operatorname{coker} \varphi_v}{\#\ker \varphi_v}$$

runs over all places v of K and is called the *local quotient*. It is in fact a finite product, since $\#\operatorname{coker} \varphi_v = \#\ker \varphi_v$ for all but finitely many v, as is recalled in Corollary 2.2.11. In the next two sections, we study $\#\operatorname{coker} \varphi_v / \#\ker \varphi_v$ for finite places $v \in M_K^0$. Firstly, for general isogenies between arbitrary abelian varieties, and secondly, for specific isogenies between elliptic curves.

2.2. Isogenies between abelian varieties over local fields

In this section we use the following notation. Let $\varphi : A \to B$ be an isogeny between two abelian varieties A and B over a number field K, and let $v \in M_K^0$ be a finite place of K. Consider the induced group homomorphism on K_v-rational points

$$\varphi_v : A(K_v) \to B(K_v).$$

Our aim is to compute the quotient $\#\operatorname{coker}\varphi_v/\#\ker\varphi_v$, which mainly consists in determining the cardinality of $\operatorname{coker}\varphi_v$, as the size of the kernel is usually obvious by the definition of φ. On a few occasions we focus on isogenies having a K_v-kernel, i.e. $A(\overline{K}_v)[\varphi] = A(K_v)[\varphi]$, and thus $\#\ker\varphi_v = \deg\varphi$ and Gal_{K_v} acts trivially on $A(\overline{K}_v)[\varphi]$. In general, the cokernel of φ_v can naturally be identified with a subgroup of $H^1(K_v, A(\overline{K}_v)[\varphi])$, since the short exact sequence of Galois modules

$$0 \longrightarrow A(\overline{K}_v)[\varphi] \longrightarrow A(\overline{K}_v) \xrightarrow{\varphi} B(\overline{K}_v) \longrightarrow 0$$

gives the long exact Galois cohomology sequence

$$0 \longrightarrow \operatorname{coker}\varphi_v \longrightarrow H^1(K_v, A(\overline{K}_v)[\varphi]) \longrightarrow \cdots$$

The next lemma determines the size of $H^1(K_v, A(\overline{K}_v)[\varphi])$ and in particular shows that it is finite. Hence $\operatorname{coker}\varphi_v$ is also finite.

Lemma 2.2.1. *Let K_v be a p-adic field and let M be a finite K_v-Galois module of order $\#M$ and with dual $M^\vee := \mathrm{Hom}(M, \mathbb{G}_m(\overline{K}_v))$. The size of the first cohomology group of M can be computed as follows.*

$$\#H^1(K_v, M) = \#H^0(K_v, M) \cdot \#H^0(K_v, M^\vee) \cdot p^{v_p(\#M)\cdot[K_v:\mathbb{Q}_p]}.$$

Proof. This follows from Theorems 2 and 5 in Chapter II.5 in [Ser02]. Define the Euler-Poincaré characteristic by $\chi(K_v, M) := \#H^0(K_v, M) \cdot \#H^2(K_v, M)/\#H^1(K_v, M)$. By the two cited theorems, we get that $\#H^2(K_v, M) = \#H^0(K_v, M^\vee)$ and that $\chi(K_v, M) = (\mathcal{O}_v : \#M\mathcal{O}_v)^{-1}$, where $\mathcal{O}_v$ is the valuation ring of K_v. Hence, $\chi(K_v, M) = p^{-v_p(\#M)\cdot[K_v:\mathbb{Q}_p]}$, which finishes the proof. □

Corollary 2.2.2. *Let φ be of prime degree ℓ. If φ or $\varphi^\vee$ has a K_v-kernel, then*

$$H^1(K_v, A(\overline{K}_v)[\varphi]) \cong \begin{cases} \mathbb{Z}/\ell\mathbb{Z}, & v \nmid \ell, \boldsymbol{\mu}_\ell \nsubseteq K_v \\ (\mathbb{Z}/\ell\mathbb{Z})^2, & v \nmid \ell, \boldsymbol{\mu}_\ell \subseteq K_v \\ (\mathbb{Z}/\ell\mathbb{Z})^{[K_v:\mathbb{Q}_p]+1}, & v|\ell, \boldsymbol{\mu}_\ell \nsubseteq K_v \\ (\mathbb{Z}/\ell\mathbb{Z})^{[K_v:\mathbb{Q}_p]+2}, & v|\ell, \boldsymbol{\mu}_\ell \subseteq K_v. \end{cases}$$

And if neither φ nor $\varphi^\vee$ has a K_v-kernel, then

$$H^1(K_v, A(\overline{K}_v)[\varphi]) \cong \begin{cases} 0, & v \nmid \ell \\ (\mathbb{Z}/\ell\mathbb{Z})^{[K_v:\mathbb{Q}_p]}, & v|\ell. \end{cases}$$

Proof. By definition $H^1(K_v, A(\overline{K}_v)[\varphi])$ is abelian and has exponent ℓ. By the previous lemma, for $M := A(\overline{K}_v)[\varphi]$, we have

$$\#H^1(K_v, M) = \begin{cases} \#H^0(K_v, M) \cdot \#H^0(K_v, M^\vee), & v \nmid \ell \\ \#H^0(K_v, M) \cdot \#H^0(K_v, M^\vee) \cdot \ell^{[K_v:\mathbb{Q}_p]}, & v \mid \ell. \end{cases}$$

If φ, respectively $\varphi^\vee$, has a K_v-kernel, then $A(\overline{K}_v)[\varphi] \cong \mathbb{Z}/l\mathbb{Z}$, respectively $\boldsymbol{\mu}_\ell$, as Galois modules. Since

$$H^0(K_v, \mathbb{Z}/\ell\mathbb{Z}) \cong \mathbb{Z}/\ell\mathbb{Z}, \text{ and } H^0(K_v, \boldsymbol{\mu}_\ell) \cong \begin{cases} 0, & \boldsymbol{\mu}_\ell \nsubseteq K_v \\ \mathbb{Z}/\ell\mathbb{Z}, & \boldsymbol{\mu}_\ell \subseteq K_v, \end{cases}$$

and $\mathbb{Z}/\ell\mathbb{Z}$ and $\boldsymbol{\mu}_\ell$ are dual to each other, we get the first statement. If neither φ nor $\varphi^\vee$ has a K_v-kernel, then neither $A(\overline{K}_v)[\varphi]$ nor its dual is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$. Therefore $H^0(K_v, A(\overline{K}_v)[\varphi]) = H^0(K_v, A(\overline{K}_v)[\varphi]^\vee) = 0$, which completes the proof. □

Corollary 2.2.3. *For p and ℓ being prime, we have*

$$H^1(\mathbb{Q}_p, \mathbb{Z}/\ell\mathbb{Z}) \cong H^1(\mathbb{Q}_p, \boldsymbol{\mu}_\ell) \cong \begin{cases} \mathbb{Z}/\ell\mathbb{Z}, & p \neq \ell \neq 2, p \not\equiv 1 \bmod \ell \\ (\mathbb{Z}/\ell\mathbb{Z})^3, & p = \ell = 2 \\ (\mathbb{Z}/\ell\mathbb{Z})^2, & \textit{otherwise}. \end{cases}$$

Proof. This is immediate from Corollary 2.2.2 upon observing that $\boldsymbol{\mu}_2 \subseteq \mathbb{Q}_p$ for all p, and $\boldsymbol{\mu}_\ell \nsubseteq \mathbb{Q}_p$ if and only if $p \not\equiv 1 \bmod \ell$ and $\ell \neq 2$. □

For a finite K_v-module M we introduce now the unramified Galois cohomology group which is an important subgroup of $H^1(K_v, M)$. Denote by K_v^{nr} the maximal unramified extension of K_v. We have that the inertia group $I_v := \mathrm{Gal}_{K_v^{\mathrm{nr}}}$ is a normal subgroup of Gal_{K_v}. Hence, the usual restriction homomorphism

$$\mathrm{Res}_{\mathrm{nr}} : H^1(K_v, M) \to H^1(K_v^{\mathrm{nr}}, M)$$

is defined, and by the Inflation-Restriction sequence its kernel is isomorphic to $H^1(\mathrm{Gal}(K_v^{\mathrm{nr}}/K_v), M^{I_v})$. We denote the kernel of $\mathrm{Res}_{\mathrm{nr}}$ by $H^1_{\mathrm{nr}}(K_v, M)$ and call it the *unramified subgroup* of $H^1(K_v, M)$. Consider again the following Galois cohomology sequence with respect to an isogeny $\varphi : A \to B$.

$$0 \longrightarrow \mathrm{coker}\, \varphi_v \xrightarrow{\delta_v} H^1(K_v, A(\overline{K}_v)[\varphi]) \longrightarrow \cdots.$$

We say that coker φ_v is *maximal*, respectively *maximally unramified*, respectively *trivial*, if δ_v is an isomorphism, respectively if δ_v induces an isomorphism between coker φ_v and the unramified subgroup $H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi])$, respectively if coker $\varphi_v = 0$. Besides merely determining the size of coker φ_v, our goal is further to specify it as a subgroup of $H^1(K_v, A(\overline{K}_v)[\varphi])$, and hence the main purpose of this subsection is to give criteria to check whether coker φ_v is maximally unramified.

Remark 2.2.4. If $K = \mathbb{Q}$ and $(p, \ell) \neq (2,2)$, the last two corollaries show that if the isogeny $\varphi : A \to B$ is of prime degree ℓ and has a $\mathbb{Q}_p$-kernel, then $H^1(\mathbb{Q}_p, A(\overline{\mathbb{Q}}_p)[\varphi])$ is either isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ or $(\mathbb{Z}/\ell\mathbb{Z})^2$. In the former case, coker φ_p is either trivial or maximal. In the latter case, there is a third possibility, namely that coker φ_p is one of the $\ell + 1$ subgroups of $H^1(\mathbb{Q}_p, A(\overline{\mathbb{Q}}_p)[\varphi])$ of order ℓ. By the next lemma, the unramified subgroup is one of these $\ell + 1$ subgroups of order ℓ.

Lemma 2.2.5. *Let K_v be a p-adic field and let M be a finite K_v-module. Then the order of $H^1_{\mathrm{nr}}(K_v, M)$ equals the order of $H^0(K_v, M)$.*

Proof. For a prime ℓ denote by $M[\ell^\infty]$ the ℓ-primary part of M, thus $M = \oplus_\ell M[\ell^\infty]$. As Galois acts on the individual $M[\ell^\infty]$, we get $H^0(K_v, \oplus_\ell M[\ell^\infty]) = \oplus_\ell H^0(K_v, M[\ell^\infty])$ and $H^1_{\mathrm{nr}}(K_v, \oplus_\ell M[\ell^\infty]) = \oplus_\ell H^1_{\mathrm{nr}}(K_v, M[\ell^\infty])$. Now apply Lemma 4.2 in [SS01] to get that the order of $H^1_{\mathrm{nr}}(K_v, M[\ell^\infty])$ equals the order of $H^0(K_v, M[\ell^\infty])$. □

We introduce some more notation. By $\tilde{A}$ we denote the reduction of A modulo v, i.e. the special fiber at v of the Néron model $\mathcal{A}/\mathcal{O}_K$ of A, and by $\tilde{A}_0(k_v)$ we denote the smooth part of the k_v-rational points of the reduction at v, i.e. the k_v-rational points of the connected component of $\tilde{A}$ intersecting the zero-section. See Theorem 1.2 of [Art86] for the existence of the Néron model $\mathcal{A}/\mathcal{O}_K$. Denote by $A_0(K_v)$ the preimage of $\tilde{A}_0(k_v)$ under the reduction-mod-v map, and by $A_1(K_v)$ the kernel of $A_0(K_v) \to \tilde{A}_0(k_v)$. We have the following two commutative diagrams with exact rows and induced group homomorphisms as vertical arrows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1(K_v) & \longrightarrow & A_0(K_v) & \longrightarrow & \tilde{A}_0(k_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_v^1} & & \downarrow{\scriptstyle \varphi_v^0} & & \downarrow{\scriptstyle \tilde{\varphi}_v^0} & & \\ 0 & \longrightarrow & B_1(K_v) & \longrightarrow & B_0(K_v) & \longrightarrow & \tilde{B}_0(k_v) & \longrightarrow & 0 \end{array} \tag{2.2}$$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_0(K_v) & \longrightarrow & A(K_v) & \longrightarrow & A(K_v)/A_0(K_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_v^0} & & \downarrow{\scriptstyle \varphi_v} & & \downarrow{\scriptstyle \overline{\varphi}_v} & & \\ 0 & \longrightarrow & B_0(K_v) & \longrightarrow & B(K_v) & \longrightarrow & B(K_v)/B_0(K_v) & \longrightarrow & 0 \end{array} \tag{2.3}$$

The vertical maps on the right, i.e. $\tilde{\varphi}_v^0$ and $\overline{\varphi}_v$, are group homomorphisms between finite groups, which follows from the theory of Néron models. Therefore, the kernels

and cokernels of $\tilde{\varphi}_v^0$ and $\overline{\varphi}_v$ are finite groups. The kernels of φ_v^0 and φ_v^1 are finite as they are subgroups of $\ker \varphi_v$, which is finite by definition. The cokernels of φ_v^0 and φ_v^1 are finite by the snake lemma, since $\operatorname{coker} \varphi_v$ is, as seen in Corollary 2.2.2. Hence, all kernels and cokernels of the vertical maps in the above two diagrams are finite groups. In the unramified case we get the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1(K_v^{\mathrm{nr}}) & \longrightarrow & A_0(K_v^{\mathrm{nr}}) & \longrightarrow & \tilde{\mathcal{A}}_0(\overline{k}_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi^1_{v,\mathrm{nr}}} & & \downarrow{\scriptstyle \varphi^0_{v,\mathrm{nr}}} & & \downarrow{\scriptstyle \tilde{\varphi}^0_{\overline{k}_v}} & & \\ 0 & \longrightarrow & B_1(K_v^{\mathrm{nr}}) & \longrightarrow & B_0(K_v^{\mathrm{nr}}) & \longrightarrow & \tilde{\mathcal{B}}_0(\overline{k}_v) & \longrightarrow & 0 \end{array} \tag{2.4}$$

We recall a basic fact, which follows from Lang's Theorem [Lan56, Theorem 1].

Lemma 2.2.6. *With notation as above, $\tilde{\mathcal{A}}_0(k_v)$ and $\tilde{B}_0(k_v)$ are finite groups of same cardinality.*

Proof. The proof is given on page 561 in [Lan56]. From the theory of Néron models it follows that $\tilde{\mathcal{A}}_0$ and $\tilde{B}_0$ are isogenous connected algebraic groups over the finite field k_v. Let G/k be a connected algebraic group over the finite field k of size q. Denote the group law by multiplication and define the Lang isogeny $f_G(g) := g^{-1}g^{(q)}$, for $g \in G(\overline{k})$, where $g^{(q)}$ is the image of g under the Frobenius morphism. Lang's Theorem [Lan56, Corollary of Theorem 1] says that $f_G : G(\overline{k}) \to G(\overline{k})$ is indeed an isogeny with kernel equal to the k-rational points of G. Now let $\varphi : G \to H$ be an isogeny between connected algebraic groups G and H over k. Then $f_H \circ \varphi = \varphi \circ f_G$, and hence the kernels of f_G and f_H have the same cardinality, which proves the lemma. □

Now we apply the snake lemma on Diagrams (2.2) and (2.3) to get a basic lemma. Recall, that the quantity $c_{A,v}$ is defined as the order of the quotient group $A(K_v)/A_0(K_v)$ and is called the *local Tamagawa number* of A at v.

Lemma 2.2.7. *With notation as above, we have the equality*

$$\frac{\#\operatorname{coker} \varphi_v}{\#\ker \varphi_v} = \frac{\#\operatorname{coker} \varphi_v^1}{\#\ker \varphi_v^1} \cdot \frac{c_{B,v}}{c_{A,v}}.$$

Proof. We have already seen the finiteness of all appearing kernels and cokernels. Applying the snake lemma on the kernels and cokernels in Diagram (2.2) we get

$$\frac{\#\ker \varphi_v^1}{\#\operatorname{coker} \varphi_v^1} \cdot \frac{\#\ker \tilde{\varphi}_v^0}{\#\operatorname{coker} \tilde{\varphi}_v^0} = \frac{\#\ker \varphi_v^0}{\#\operatorname{coker} \varphi_v^0}.$$

Since $\#\tilde{\mathcal{A}}_0(k_v) = \#\tilde{B}_0(k_v)$, by Lemma 2.2.6, we get $\#\ker \tilde{\varphi}_v^0 = \#\operatorname{coker} \tilde{\varphi}_v^0$. It follows that $\#\ker \varphi_v^1/\#\operatorname{coker} \varphi_v^1 = \#\ker \varphi_v^0/\#\operatorname{coker} \varphi_v^0$. Applying the snake lemma on Diagram (2.3) gives

$$\frac{\#\operatorname{coker} \varphi_v}{\#\ker \varphi_v} = \frac{\#\operatorname{coker} \varphi_v^0}{\#\ker \varphi_v^0} \cdot \frac{\#\operatorname{coker} \overline{\varphi}_v}{\#\ker \overline{\varphi}_v}.$$

By definition, we have $\#\operatorname{coker} \overline{\varphi}_v/\#\ker \overline{\varphi}_v = c_{B,v}/c_{A,v}$, which completes the proof. □

We continue by examining the quotient $\#\operatorname{coker}\varphi_v^1/\#\ker\varphi_v^1$. We start by recalling two basic lemmas, and then we deduce the well known fact that this quotient is almost always trivial, since φ_v^1 is an isomorphism for all but finitely many places v.

Lemma 2.2.8. *The kernel of reduction $A_1(K_v)$ is a pro-p group.*

Proof. We have that $A_1(K_v)$ is isomorphic to the group $\hat{A}(\mathfrak{m}_v)$ associated to the formal group $\hat{A}$ of A defined over the valuation ring $\mathcal{O}_v$ of K_v with maximal ideal $\mathfrak{m}_v$. If an integer n is coprime to the characteristic p of the residue field k_v, then the multiplication-by-n endomorphism on $\hat{A}(\mathfrak{m}_v)$ is an isomorphism. It is an easy exercise to check that a profinite group is in fact a pro-p group provided that the multiplication-by-ℓ map is an isomorphism for all primes $\ell \neq p$. Hence $A_1(K_v)$ is a pro-p group. □

Lemma 2.2.9. *If $v \nmid \deg\varphi$, then φ_v^1 and $\varphi_{v,\mathrm{nr}}^1$ are isomorphisms.*

Proof. Denote the degree of φ by n. There exist isogenies $\psi : B \to A$ and $\phi : A \to B$, such that $\psi \circ \varphi : A \to A$ and $\phi \circ \psi : B \to B$ are the multiplication-by-n maps $[n]$. Hence we get the following induced group homomorphisms on the kernels of reduction.

$$A_1(K_v) \xrightarrow{\varphi_v^1} B_1(K_v) \xrightarrow{\psi_v^1} A_1(K_v) \xrightarrow{\phi_v^1} B_1(K_v)$$

with $[n]_v^1 : A_1(K_v) \to A_1(K_v)$ and $[n]_v^1 : B_1(K_v) \to B_1(K_v)$.

Since $v \nmid \deg\varphi$, we have by the previous lemma that both maps $[n]_v^1$ are isomorphisms. Hence it follows that all three homomorphisms ψ_v^1, ϕ_v^1 and φ_v^1 are isomorphisms. Now for any finite unramified extension L_w/K_v, we get by the same argument that φ_w^1 is an isomorphism, and so also is $\varphi_{v,\mathrm{nr}}^1$. □

Corollary 2.2.10. *If a prime ℓ divides the cardinality of a kernel or cokernel of one of the induced group homomorphisms φ_v, φ_v^0, φ_v^1, $\overline{\varphi}_v$ or $\tilde{\varphi}_v^0$ appearing in Diagrams (2.2) and (2.3), or ℓ divides the Tamagawa quotient $c_{B,v}/c_{A,v}$, then $\ell \mid \deg\varphi$. Further, if $\gcd(\deg\varphi, c_{A,v} \cdot c_{B,v}) = 1$, then $\overline{\varphi}_v$ is an isomorphism.*

In particular, if φ is of prime degree ℓ, then the cardinalities of all kernels and cokernels of φ_v, φ_v^0, φ_v^1, $\overline{\varphi}_v$ and $\tilde{\varphi}_v^0$, as well as the Tamagawa quotient $c_{B,v}/c_{A,v}$, are powers of ℓ.

Proof. By construction, the claim is clear for all the kernels. If φ is the multiplication-by-n endomorphism of A for a positive integer n, then this is also clear for the cokernels. For a general isogeny φ of degree n, as mentioned in the proof of the above lemma, there is an isogeny $\psi : B \to A$, such that $[n] = \psi \circ \varphi$. From the exact sequence

$$0 \to \ker\psi/\varphi(\ker[n]) \to \operatorname{coker}\varphi \to \operatorname{coker}[n] \to \operatorname{coker}\psi \to 0$$

we derive the statement about the cokernels of the homomorphisms induced by φ. Use Lemma 2.2.7 to get the statement about the Tamagawa quotient.

Now assume that $\gcd(\deg\varphi, c_{A,v}\cdot c_{B,v}) = 1$. If a prime ℓ divides the Tamagawa quotient $c_{B,c}/c_{A,v}$ then $\ell \mid \deg\varphi$ by the above part of this lemma, hence ℓ does not divide the product $c_{A,v}\cdot c_{B,v}$. Therefore there are no primes ℓ dividing $c_{B,c}/c_{A,v}$ and thus $c_{A,v} = c_{B,v}$. This implies $\#\ker\overline{\varphi}_v = \#\operatorname{coker}\overline{\varphi}_v$. If a prime ℓ divides $\#\ker\overline{\varphi}_v$, then ℓ divides $\deg\varphi$ and $c_{A,v}$, hence there are no such primes ℓ and $\overline{\varphi}_v$ is an isomorphism. □

We conclude that the product over all quotients $\#\operatorname{coker}\varphi_v/\#\ker\varphi_v$ is actually a finite product. Let S be a finite subset of M_K containing the infinite places, the places of bad reduction of A and B and the places dividing the degree of the isogeny φ.

Corollary 2.2.11. *If $v \nmid \deg\varphi$ and v is a place of good reduction, then*

$$\frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v} = 1; \;\; \textit{thus} \;\; \prod_{v\in M_K}\frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v} = \prod_{v\in S}\frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v}.$$

Proof. Combine Lemmas 2.2.7 and 2.2.9 with the fact that the Tamagawa quotient equals 1 in case of good reduction. □

In view of the corollary, the goal of this section is to provide methods to compute the quotient $\#\operatorname{coker}\varphi_v/\#\ker\varphi_v$, in case v is a place of bad reduction or $v \mid \deg\varphi$. If we stick to good reduction, but do not care whether v divides the degree of φ, then the next lemma gives a very nice criterion to check whether $\operatorname{coker}\varphi_v$ is maximally unramified. The notation used in part (i) of the lemma comes from the following diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1(\overline{K}_v) & \longrightarrow & A_0(\overline{K}_v) & \longrightarrow & \tilde{\mathcal{A}}_0(\overline{k}_v) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi^1_{\overline{K}_v}} & & \downarrow{\scriptstyle \varphi^0_{\overline{K}_v}} & & \downarrow{\scriptstyle \tilde{\varphi}^0_v} & & \\ 0 & \longrightarrow & B_1(\overline{K}_v) & \longrightarrow & B_0(\overline{K}_v) & \longrightarrow & \tilde{\mathcal{B}}_0(\overline{k}_v) & \longrightarrow & 0 \end{array}$$

Lemma 2.2.12 (Criterion for maximal unramifiedness of $\operatorname{coker}\varphi_v$ in case v is a place of good reduction)**.** *Assume v is a place of good reduction.*

(i) If $\ker\varphi^1_{\overline{K}_v}$ is trivial, then $\operatorname{coker}\varphi_v$ is maximally unramified.

(ii) If φ has a K_v-kernel and φ^1_v is injective, then $\operatorname{coker}\varphi_v$ is maximally unramified.

Proof. Part (ii) for $K_v = \mathbb{Q}_p$, $\deg\varphi$ being an odd prime, and A and B are elliptic curves, is Lemma A.3 in the Appendix of [Dok05] by Tom Fisher. In general, (ii) follows directly from (i), as the assumptions imply that $\ker\varphi^1_{\overline{K}_v} = \ker\varphi^1_v = 0$.

For part (i) note, that if $[\xi] \in H^1(K_v, A[\varphi])$ is an element of $\operatorname{coker}\varphi_v$, then $[\xi]$ lies in the kernel of $H^1(K_v, A[\varphi]) \to H^1(K_v, A)$. This means that there is a point $P \in A(\overline{K}_v)$, such that $\xi(\sigma) = P^\sigma - P$, for all $\sigma \in \mathrm{Gal}_{K_v}$. As v is a place of good reduction we get that $P \in A_0(\overline{K}_v)$. Consider the reduction-mod-v map $A_0(\overline{K}_v) \to \tilde{\mathcal{A}}_0(\overline{k}_v)$, which is a group homomorphism. Hence, $\overline{P^\tau - P} = \overline{P}^\tau - \overline{P} = \mathcal{O}$, for all $\tau \in I_v$, as I_v acts trivially on $\mathcal{A}_0(\overline{k}_v)$. Therefore for all $\tau \in I_v$, $P^\tau - P$ lies in the kernel of reduction $\varphi^1_{\overline{K}_v}$. As $\varphi^1_{\overline{K}_v}$ is assumed to be trivial we immediately deduce that $P^\tau - P = \mathcal{O}$, for all $\tau \in I_v$, which is equivalent to $P \in A_0(K_v^{\mathrm{nr}})$. By definition, $[\xi]$ lies in $H^1_{\mathrm{nr}}(K_v, A[\varphi])$ if it is in the kernel

of $\mathrm{Res}_{\mathrm{nr}}$. This is clearly the case if $P \in A(K_v^{\mathrm{nr}})$, because this makes the restriction of ξ to I_v to be the zero map, and thus coker φ_v injects into $H^1_{\mathrm{nr}}(K_v, A[\varphi])$.

By Lemmas 2.2.5 and 2.2.7, coker φ_v also surjects onto $H^1_{\mathrm{nr}}(K_v, A[\varphi])$, as its order is at least the order of $H^1_{\mathrm{nr}}(K_v, A[\varphi])$. □

We continue with presenting a reinterpretation of the quotient $\#\operatorname{coker}\varphi_v^1/\#\ker\varphi_v^1$ given by Schaefer in [Sch96]. Using these results, it is very easy to compute $\#\operatorname{coker}\varphi_v^1/\#\ker\varphi_v^1$ for elliptic curves. First we need some notation. Assume that the abelian varieties A and B are of dimension d and let $v \in M_K^0$ be a finite place. It is possible to write the isogeny $\varphi : A \to B$ as a d-tuple of power series in d-variables in a neighbourhood of the identity element $\mathcal{O}$. Let $|\varphi'(0)|_v$ be the normalised v-adic absolute value of the determinant of the Jacobian matrix of partial derivatives of such a power series representation of φ evaluated at 0. Note that $|\varphi'(0)|_v$ is well defined.

Proposition 2.2.13. *With notation as above,*

$$|\varphi'(0)|_v^{-1} = \frac{\#\operatorname{coker}\varphi_v^1}{\#\ker\varphi_v^1};\ \textit{hence}\ \ |\varphi'(0)|_v = 1,\ \textit{if}\ v \nmid \deg\varphi.$$

Proof. Combine [Sch96, Lemma 3.8] with Lemmas 2.2.7 and 2.2.9. □

Corollary 2.2.14. *With notation as above,*

$$\frac{\#\operatorname{coker}\varphi_v}{\#\ker\varphi_v} = |\varphi'(0)|_v^{-1} \cdot \frac{c_{B,v}}{c_{A,v}}.$$

Proof. This follows from the last proposition together with Lemma 2.2.7. □

Remark 2.2.15. In the case of elliptic curves, $\varphi'(0)$ is just the leading coefficient of the power series representation of φ. One can easily compute this value: Use Vélu's algorithm [Vél71] to describe φ as coordinate functions $\varphi(X,Y) = (\tilde{X}(X,Y), \tilde{Y}(X,Y))$ and then write $-\tilde{X}/\tilde{Y}$ as a power series in $Z := -X/Y$, see [Sil86, IV]. We do this explicitly in Propositions 3.3.2 and 3.3.10.

Before we present our main criterion for checking that coker φ_v is maximally unramified, we give a basic lemma about $|\varphi'(0)|_v$ and the maps φ_v^1 and $\varphi_{v,\mathrm{nr}}^1$. The aim of the lemma is to provide a way to replace $v \nmid \deg\varphi$ with the weaker assumption $e_v < p-1$, where e_v is the ramification index of the place v of K. Note, that if $K_v = \mathbb{Q}_p$ and $p \neq 2$, then the condition about the ramification index is fulfilled, i.e. we have $e_v < p-1$.

Lemma 2.2.16. *With notation as above, the following holds.*

(i) If $|\varphi'(0)|_v = 1$ and $\varphi_{v,\mathrm{nr}}^1$ is injective, then φ_v^1 and $\varphi_{v,\mathrm{nr}}^1$ are isomorphisms. Hence, if φ_v^1 and $\varphi_{v,\mathrm{nr}}^1$ are injective, then φ_v^1 and $\varphi_{v,\mathrm{nr}}^1$ are isomorphisms if and only if $|\varphi'(0)|_v = 1$.

(ii) If the ramification index $e_v < p-1$, then φ_v^1 and $\varphi_{v,\mathrm{nr}}^1$ are injective.

(iii) If $K = \mathbb{Q}$, then φ_p^1 and $\varphi_{p,\mathrm{nr}}^1$ are injective, unless $p = 2$ and $2 \mid \deg\varphi$.

(iv) If $K = \mathbb{Q}$ and $|\varphi'(0)|_v = 1$, then φ_v^1 and $\varphi_{v,\mathrm{nr}}^1$ are isomorphisms, unless $p = 2$ and $2 \mid \deg\varphi$.

Proof. Assume $|\varphi'(0)|_v = 1$, thus $|\varphi'(0)|_w = 1$ for all unramified finite field extensions L_w/K_v. Since $\varphi^1_{v,\mathrm{nr}}$ is injective, the maps $\varphi^1_w : A_1(L_w) \to B_1(L_w)$ are also injective. By Proposition 2.2.13, the size of the kernels and cokernels of φ^1_w agree and therefore all φ^1_w are isomorphisms. Hence $\varphi^1_{v,\mathrm{nr}}$ is an isomorphism, which proves (i).

For (ii) use the isomorphism $A_1(K_v) \cong \hat{A}(\mathfrak{m}_v)$. Then use [Sil86, IV. Theorem 6.1] or the next lemma to conclude that φ^1_w is injective for any finite unramified field extension L_w/K_v. Hence $\varphi^1_{v,\mathrm{nr}}$ is injective.

For (iii) apply (ii) in case $p \neq 2$. In case $2 \nmid \deg \varphi$, this is due to Lemma 2.2.9. Combing part (i) and part (iii) gives part (iv). □

Lemma 2.2.17. *With notation as above, if the ramification index $e_v < p-1$ then the reduction-mod-v map $A_0(K_v) \to \tilde{\mathcal{A}}_0(k_v)$ has torsion-free kernel, i.e. $A_1(K_v)$ is torsion-free. In particular, this gives an injection $A(K)_{\mathrm{tors}} \hookrightarrow \tilde{\mathcal{A}}_0(k_v)$, thus if in addition v is a place of good reduction there is an injection $A(K)_{\mathrm{tors}} \hookrightarrow \tilde{\mathcal{A}}(k_v)$.*

Proof. This is essentially the content of the Appendix of [Kat81]. □

The next lemma and theorem are a slight generalisation of Lemmas 4.3 and 4.5 of [SS01]. Theorem 2.2.19 provides our main criterion to check whether $\operatorname{coker} \varphi_v$ is maximally unramified. To state the lemma we introduce the map

$$\delta^0_v : \operatorname{coker} \varphi^0_v \to H^1(K_v, A(\overline{K}_v)[\varphi]).$$

It is obtained by composing the natural map $\operatorname{coker} \varphi^0_v \to \operatorname{coker} \varphi_v$ from Diagram (2.3) with the connecting homomorphism $\delta_v : \operatorname{coker} \varphi_v \to H^1(K_v, A(\overline{K}_v)[\varphi])$. Since $\operatorname{coker} \varphi^0_v \to \operatorname{coker} \varphi_v$ need not be injective, δ^0_v may also not be injective. Similarly one defines the map

$$\delta^0_{v,\mathrm{nr}} : \operatorname{coker} \varphi^0_{v,\mathrm{nr}} \to H^1(K^{\mathrm{nr}}_v, A(\overline{K}_v)[\varphi]).$$

Lemma 2.2.18. *If $\varphi^1_{v,\mathrm{nr}}$ is surjective, then the image of $\operatorname{coker} \varphi^0_v$ under δ^0_v lies in $H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi])$.*

Proof. In the above Diagram (2.4), the first vertical map $\varphi^1_{v,\mathrm{nr}}$ is surjective by assumption. The third vertical map $\tilde{\varphi}^0_{\bar{k}_v}$ is surjective, since $\bar{k}_v$ is algebraically closed, therefore the middle vertical map $\varphi^0_{v,\mathrm{nr}}$ is also surjective, i.e. $\operatorname{coker} \varphi^0_{v,\mathrm{nr}}$ is trivial. The following diagram commutes.

$$\begin{array}{ccc} \operatorname{coker} \varphi^0_v & \xrightarrow[\delta^0_v]{} & H^1(K_v, A(\overline{K}_v)[\varphi]) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Res}_{\mathrm{nr}}} \\ \operatorname{coker} \varphi^0_{v,\mathrm{nr}} & \xrightarrow[\delta^0_{v,\mathrm{nr}}]{} & H^1(K^{\mathrm{nr}}_v, A(\overline{K}_v)[\varphi]) \end{array}$$

As the lower left group is trivial, the image of the upper left group in the lower right group must be trivial, i.e. the image of δ^0_v lies in $H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi])$. □

Theorem 2.2.19 (Main criterion for maximal unramifiedness of coker φ_v)**.** *Let $\varphi : A \to B$ be an isogeny between two abelian varieties A and B over a number field K, and let $v \in M_K^0$ be a finite place of K. If $\varphi^1_{v,\mathrm{nr}}$ is surjective and φ^1_v and $\overline{\varphi}_v$ are isomorphisms, then* coker φ_v *is maximally unramified.*

Proof. As $\overline{\varphi}_v$ is an isomorphism, coker $\varphi^0_v \to$ coker φ_v is also an isomorphism. Hence by the above lemma, coker φ_v maps injectively onto a subgroup of $H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi])$. We complete the proof by showing that these two groups have same cardinality. By Lemmas 2.2.5 and 2.2.7, we get $\#H^1_{\mathrm{nr}}(K_v, A(\overline{K}_v)[\varphi]) = \#\ker \varphi_v = \#\operatorname{coker} \varphi_v$. □

Our assumptions on φ^1_v and $\varphi^1_{v,\mathrm{nr}}$ in Lemma 2.2.18 and Theorem 2.2.19 replaced the assumption $v \nmid \deg \varphi$ in Lemmas 4.3 and 4.5 of [SS01]. As seen in Lemma 2.2.9, $v \nmid \deg \varphi$ is a stronger assumption, hence we easily deduce the result of Schaefer and Stoll.

Corollary 2.2.20 (Criterion for maximal unramifiedness of coker φ_v in case $v \nmid \deg \varphi$)**.** *If $v \nmid \deg \varphi$ and* $\gcd(\deg \varphi, c_{A,v} \cdot c_{B,v}) = 1$ *then* coker φ_v *is maximally unramified.*

Proof. This is Lemma 4.5 of [SS01]. The corollary follows directly from Theorem 2.2.19 together with Lemma 2.2.9 and Corollary 2.2.10. □

We also want to apply Theorem 2.2.19 in case $v \mid \deg \varphi$. As seen in Lemma 2.2.16, we may replace $v \nmid \deg \varphi$ with the conditions $e_v < p - 1$ and $|\varphi'(0)|_v = 1$.

Corollary 2.2.21 (Criteria for maximal unramifiedness of coker φ_v in case $v \mid \deg \varphi$)**.** *Assume that the ramification index $e_v < p - 1$.*

(i) If $|\varphi'(0)|_v = 1$ and $\gcd(\deg \varphi, c_{A,v} \cdot c_{B,v}) = 1$*, then* coker φ_v *is maximally unramified.*

(ii) If v is a place of good reduction, then coker φ_v *is maximally unramified if and only if $|\varphi'(0)|_v = 1$.*

(iii) If v is a place of good reduction and φ has a K_v-kernel, then $|\varphi'(0)|_v = 1$ and coker φ_v *is maximally unramified.*

Proof. For part (i) combine Lemma 2.2.16 with Theorem 2.2.19 and Corollary 2.2.10. For part (ii) note, that $c_{A,v} = c_{B,v} = 1$. Hence, if $|\varphi'(0)|_v = 1$, then by (i) we get that coker φ_v is maximally unramified. Now assume that coker φ_v is maximally unramified, hence $\#\operatorname{coker} \varphi_v = \#\ker \varphi_v$. By Corollary 2.2.14 we get that $|\varphi'(0)|_v = c_{B,v}/c_{A,v} = 1$, which completes (ii). For (iii), combine (ii) with Lemmas 2.2.12 and 2.2.16. □

We summarise all the criteria for maximal unramifiedness for the case that $K = \mathbb{Q}$. The first one is easily applicable when A and B are elliptic curves.

Corollary 2.2.22 (Criteria for maximal unramifiedness of coker φ_p in case $K = \mathbb{Q}$)**.** *Let $\varphi : A \to B$ be an isogeny between two abelian varieties A and B over $\mathbb{Q}$ and let p be a prime such that $p \neq 2$ if $2 \mid \deg \varphi$.*

(i) If $|\varphi'(0)|_p = 1$ and $\gcd(\deg \varphi, c_{A,p} \cdot c_{B,p}) = 1$*, then* coker φ_p *is maximally unramified.*

(ii) If p is a place of good reduction and φ has a $\mathbb{Q}_p$-kernel, then $|\varphi'(0)|_p = 1$ and coker φ_p *is maximally unramified.*

Proof. Follows directly from Lemma 2.2.16, Theorem 2.2.19, and Corollary 2.2.21. □

We end this section with a basic lemma about the infinite places.

Lemma 2.2.23. *Let L be either $\mathbb{R}$ or $\mathbb{C}$ and let A and B be abelian varieties over L. For an isogeny $\varphi : A \to B$ denote with $\varphi_\infty : A(L) \to B(L)$ the induced group homomorphism on L-rational points.*

(i) If $L = \mathbb{C}$, then $\#\operatorname{coker}\varphi_\infty / \#\ker\varphi_\infty = 1/\deg\varphi$.

(ii) If $L = \mathbb{R}$, then $\#\operatorname{coker}\varphi_\infty = 1$, if $2 \nmid \deg\varphi$.

Proof. Part (i) is obvious, as $\mathbb{C}$ is algebraically closed and of characteristic 0, hence φ_∞ is surjective and the size of the kernel equals the degree. For (ii) note, that $\operatorname{coker}\varphi_\infty$ embeds into $H^1(\mathbb{R}, A[\varphi])$, which is trivial if the order of $\mathrm{Gal}_\mathbb{R}$ is coprime to $A[\varphi]$. □

In the next section we consider the special case of A and B being elliptic curves E and E' and the isogeny being of prime degree ℓ and having a K_v-kernel. Isogenies between elliptic curves are usually denoted by η. As before we are interested in whether $\operatorname{coker}\eta_v$ is maximal, maximally unramified, or trivial. The goal is to classify $\operatorname{coker}\eta_v$ with respect to the reduction type at v. To show maximal unramifiedness we use the criteria established above. Further, to see whether $\operatorname{coker}\eta_v$ is trivial or maximal we use the equation

$$\#\operatorname{coker}\eta_v = \ell \cdot |\eta'(0)|_v^{-1} \cdot \frac{c_{E',v}}{c_{E,v}}$$

from Lemma 2.2.14. In any case, we want to have a way to compute $|\eta'(0)|_v$ and the Tamagawa numbers $c_{E',v}$ and $c_{E,v}$ with respect to the reduction type at v.

2.3. Isogenies of prime degree between elliptic curves over local fields

The notation for this section is the following. Fix two prime numbers p and ℓ. It is possible that $p = \ell$. Let E and E' be elliptic curves over a p-adic field K_v and let $\eta : E \to E'$ be an isogeny of prime degree ℓ. We use the notations from Diagrams (2.2), (2.3), and (2.4) with $E = A$ and $E' = B$. Assuming that η has a K_v-kernel, i.e. $E(\overline{K}_v)[\eta] = E(K_v)[\eta]$, the goal of this section is to determine under which further assumptions the reduction type of E at v determines whether $\operatorname{coker}\eta_v$ is maximal, maximally unramified, or trivial. In the case when $K_v = \mathbb{Q}_p$ and $\ell \geq 5$, we can give a complete classification, which is stated in our main Theorem 2.3.7. If the reduction type at p is not additive, then we can give partial answers for the two cases $\ell = 2$ and $\ell = 3$.

We start with computing the quotient $c_{E'}/c_E$ of Tamagawa numbers with respect to the reduction type at v. In most cases the Tamagawa quotient of isogenous elliptic curves can easily be computed with Tate's algorithm and the theory of Tate curves. See for example the Appendix of [Dok05] by Tom Fisher or [DD13, §6 and §9] by Tim and Vladimir Dokchitser.

Lemma 2.3.1. *Suppose that E/K_v has either good reduction, or non-split multiplicative reduction and $\ell \neq 2$, or additive reduction and $\ell \geq 5$. Then the group homomorphism $\overline{\eta}_v$ is an isomorphism, and hence $c_{E'}/c_E = 1$.*

Proof. In case of good reduction this is clear, since $c_{E,v} = c_{E',v} = 1$. From Tate's algorithm [Tat75] it follows that $c_{E,v}$ and $c_{E',v}$ are at most 4 in the additive case, and at most 2 in the non-split multiplicative case. Hence $\gcd(\deg \eta, c_{E,v} \cdot c_{E',v}) = 1$, and the result follows directly from Corollary 2.2.10. □

To calculate the Tamagawa quotient in the case of split multiplicative reduction we use the theory of Tate curves.

Theorem 2.3.2. (Tate) *Assume that E/K_v has split multiplicative reduction. Then there is a unique $q \in K_v^*$, s.t. $v(q) > 0$, and we have the following Galois equivariant p-adic analytic isomorphism*

$$E(L) \cong L^*/q^{\mathbb{Z}},$$

for all algebraic field extension L/K_v. Moreover, $c_{E,v} = v(q)$.

Proof. See [Sil94, V Theorem 5.3]. The last statement follows from the proof of the surjectivity of the Tate map [Sil94, V.4]. □

Remark 2.3.3. If E/K_v is an elliptic curve having split multiplicative reduction, we have $E(\overline{K}_v) \cong \overline{K}_v^*/q^{\mathbb{Z}}$, for $q \in K_v^*$ and $v(q) > 0$. We want to classify which Galois invariant subgroups of prime order ℓ exist and whether they are contained in the connected component of the identity $E_0(\overline{K}_v) \cong \overline{K}_v^*$. Since they are all subgroups of $E(\overline{K}_v)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, there are at most $\ell + 1$ of such groups. The ℓ-th roots of unity $\{\xi_\ell, \xi_\ell^2, \ldots, \xi_\ell^{\ell-1}, 1\}$ in $\overline{K}_v^*$ form a Galois invariant subgroup of $\overline{K}_v^*/q^{\mathbb{Z}}$, which is contained in the connected component of the identity, and a generator is defined over K_v if and only if $\boldsymbol{\mu}_\ell \subseteq K_v$. Hence this subgroup of $E(\overline{K}_v)[\ell]$ is isomorphic to $\boldsymbol{\mu}_\ell$ as a Galois module. The remaining ℓ subgroups are defined over $K_v(\sqrt[\ell]{q}, \boldsymbol{\mu}_\ell)$. None of these ℓ subgroups are contained in the connected component of the identity. They are generated by $\xi_\ell^i \sqrt[\ell]{q}$, for $i = 0, \ldots, \ell - 1$. The elements of such a subgroup have different minimal polynomials, hence if the subgroup is Galois invariant, then it is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ as a Galois module.

Lemma 2.3.4. *With notation as above, if E/K_v has split multiplicative reduction, then*

$$\frac{c_{E'}}{c_E} = \begin{cases} 1/\ell, & \ker \eta_v \nsubseteq E_0(\overline{K}_v) \\ \ell, & \ker \eta_v \subseteq E_0(\overline{K}_v). \end{cases}$$

Proof. This is Lemma A.2 of the appendix of [Dok05] by Tom Fisher. To identify our lemma with Lemma A.2, use the last remark to see that $\ker \eta_v \nsubseteq E_0(\overline{K}_v)$ implies that $\ker \eta_v \cong \mathbb{Z}/\ell\mathbb{Z}$, and $\ker \eta_v \subseteq E_0(\overline{K}_v)$ implies that $\ker \eta_v \cong \boldsymbol{\mu}_\ell$ as Galois modules.

We give now a slightly longer version of Tom Fisher's proof. By theorem 2.3.2 we have $E(\overline{K}_v) \cong \overline{K}_v^*/q_1^{\mathbb{Z}}$ and $E'(\overline{K}_v) \cong \overline{K}_v^*/q_2^{\mathbb{Z}}$. If $\ker \eta_v \nsubseteq E_0(\overline{K}_v)$, then $\ker \eta_v = \langle [\xi_\ell^i \sqrt[\ell]{q_1}] \rangle$, for an $i \in \{0, \ldots, \ell - 1\}$, and $\eta_v : \overline{K}_v^*/q_1^{\mathbb{Z}} \to \overline{K}_v^*/q_2^{\mathbb{Z}}$ is given by $[x] \mapsto [x]$ and $q_2 = \xi_\ell^i \sqrt[\ell]{q_1}$. Therefore $c_{E'}/c_E = v(q_2)/v(q_1) = v(\xi_\ell^i \sqrt[\ell]{q_1})/v(q_1) = 1/\ell$.

If $\ker \eta_v \subseteq E_0(\overline{K}_v)$, then $\ker \eta_v = \langle [\xi_\ell] \rangle$, and $\eta_v : \overline{K}_v^*/q_1^{\mathbb{Z}} \to \overline{K}_v^*/q_2^{\mathbb{Z}}$ is given by $[x] \mapsto [x^\ell]$ and $q_2 = q_1^\ell$. Therefore $c_{E'}/c_E = v(q_2)/v(q_1) = v(q_1^\ell)/v(q_1) = \ell$. □

Now we study the implications of $\ker \eta_v$ being or not being part of the connected component of the identity $E_0(\overline{K}_v)$. The result is essentially a corollary of Tate's algorithm [Tat75] and explores the fact that η is of prime degree ℓ.

Lemma 2.3.5. *With notation as above, we have:*
(i) If $\ker \eta_v \not\subseteq E_0(\overline{K}_v)$*, then* η *has a* K_v*-kernel,* η_v^1 *is an isomorphism,* $|\eta'(0)|_v = 1$*,* $\ell \mid c_E$*, and exactly one of the following three cases holds.*

- *E has split multiplicative reduction,*
- *E has non-split multiplicative reduction and* $\ell = 2$*,*
- *E has additive reduction and either* $\ell = 2$ *or* $\ell = 3$*.*

(ii) If $\ker \eta_v \subseteq E_0(\overline{K}_v)$*, assume additionally that* η *has a* K_v*-kernel and that* η_v^1 *is injective. We have the following implications.*

- *E has multiplicative reduction* $\Rightarrow\ v \nmid \ell$ *and* $|\eta'(0)|_v = 1$*,*
- *E has split multiplicative reduction* $\Rightarrow\ \boldsymbol{\mu}_\ell \subseteq K_v$*,*
- *E has non-split multiplicative reduction and* $\ell \neq 2 \Rightarrow\ \boldsymbol{\mu}_\ell \not\subseteq K_v$*,*
- *E has additive reduction* $\Rightarrow\ v \mid \ell$*.*

Proof. If $\ker \eta_v$ is trivial, then it is clearly contained in $E_0(\overline{K}_v)$. Hence $\ker \eta_v \not\subseteq E_0(\overline{K}_v)$ implies that $\ker \eta_v$ is non-trivial, and therefore η has a K_v-kernel as its degree is prime. It also implies that $\eta^0_{\overline{K}_v}$, η_v^0, and thus η_v^1 are injective. From the triviality of $\eta^0_{\overline{K}_v}$ is follows that $H^1(K_v, E_0(\overline{K}_v)[\eta])$ is trivial and hence $\operatorname{coker} \eta_v^0$ is also trivial. We deduce that η_v^0 is an isomorphism, and therefore $\tilde{\eta}_v^0$ is surjective. By Lemma 2.2.6, $\tilde{\eta}_v^0$ is an isomorphism, as its kernel and cokernel have equal cardinalities. This immediately implies that η_v^1 is an isomorphism, which gives $|\eta'(0)|_v = 1$, by Proposition 2.2.13. Again by the fact that η_v^0 is an isomorphism, it follows that $\#\ker \overline{\eta}_v = \ell$, which gives that ℓ divides the Tamagawa number c_E. In particular, the reduction type is bad. By [Tat75], c_E is ≤ 2 in the non-split multiplicative case and ≤ 4 in the additive case, giving (i).

For (ii) let $P \in E(K_v)$ be a generator of $\ker \eta_v$. If $\ker \eta_v \subseteq E_0(\overline{K}_v)$ and η has a K_v-kernel, then P generates $\ker \eta_v^0$. Since we assumed η_v^1 to be injective, the order of $\overline{P}$ is ℓ. Set $|k_v| =: p^f$. The order of $\overline{P}$ divides the cardinality of $\tilde{\mathcal{E}}_0(k_v)$, which is either $p^f - 1$, $p^f + 1$, or p^f, depending on whether the reduction type is split multiplicative, non-split multiplicative, or additive, respectively [Tat75, §7]. Therefore, we get the implications

- multiplicative $\Rightarrow\ p^f \not\equiv 0(\ell)\ \Rightarrow\ p \neq \ell\ \Rightarrow\ v \nmid \ell$,
- split $\Rightarrow\ p^f \equiv 1(\ell)\ \Rightarrow\ \boldsymbol{\mu}_\ell \subseteq k_v\ \Rightarrow\ \boldsymbol{\mu}_\ell \subseteq K_v$,
- non-split and $\ell \neq 2 \Rightarrow\ p^f \not\equiv 0, 1(\ell) \Rightarrow\ \boldsymbol{\mu}_\ell \not\subseteq k_v \Rightarrow\ \boldsymbol{\mu}_\ell \not\subseteq K_v$,
- additive $\Rightarrow\ p^f \equiv 0(l)\ \Rightarrow\ p = \ell,\ \Rightarrow\ v \mid \ell$.

By Proposition 2.2.13, $v \nmid \ell$ implies $|\eta'(0)|_v = 1$, which completes (ii). □

We summarise the results and state under which further assumptions $\operatorname{coker} \eta_v$ is trivial, maximally unramified, or maximal in the case of multiplicative reduction.

Corollary 2.3.6 (Criteria to classify $\operatorname{coker} \eta_v$ is case of multiplicative reduction)**.** *(i) If the reduction type of E/K_v is split multiplicative and $\ker \eta_v \not\subseteq E_0(\overline{K}_v)$, then $|\eta'(0)|_v = 1$ and $\operatorname{coker} \eta_v$ is trivial.*

(ii) If the reduction type of E/K_v is split multiplicative, $\ker \eta_v \subseteq E_0(\overline{K}_v)$, η has a K_v-kernel, and η_v^1 is injective, then $v \nmid \ell, \boldsymbol{\mu}_\ell \subseteq K_v$, $|\eta'(0)|_v = 1$, and $\operatorname{coker} \eta_v$ is maximal.

(iii) If the reduction type of E/K_v is non-split multiplicative, $\ell \neq 2$, η has a K_v-kernel, and η_v^1 is injective, then $v \nmid \ell, \boldsymbol{\mu}_\ell \not\subseteq K_v$, $|\eta'(0)|_v = 1$ and $\operatorname{coker} \eta_v$ is maximally unramified.

(iv) If the reduction type of E/K_v is non-split multiplicative, $\ell = 2$, $v \nmid \ell$, and η has a K_v-kernel, then $\boldsymbol{\mu}_\ell \subseteq K_v$ and $|\eta'(0)|_v = 1$. Further $\operatorname{coker} \eta_v$ is trivial if $c_{E'}/c_E = 1/2$, $\operatorname{coker} \eta_v$ is maximal if $c_{E'}/c_E = 2$, and $\operatorname{coker} \eta_v$ is maximally unramified if $c_E = c_{E'} = 1$.

Proof. Lemma 2.3.5 already contains everything of (i)-(iii) but the statement whether $\operatorname{coker} \eta_v$ is trivial, maximally unramified, or maximal. In (iv) we get $|\eta'(0)|_v = 1$ and $\boldsymbol{\mu}_\ell \subseteq K_v$, as $v \nmid \ell$ and $\ell = 2$. It remains to classify $\operatorname{coker} \eta_v$.

By Corollary 2.2.14, we obtain the equation $\#\operatorname{coker} \eta_v = \ell \cdot c_{E'}/c_E$, and the size of $H^1(K_v, E(\overline{K}_v)[\eta])$ is given by Corollary 2.2.3. The Tamagawa quotient in (i)-(iii) can be computed with Lemmas 2.3.1 and 2.3.4. This shows triviality of $\operatorname{coker} \eta_v$ in (i) and the first case in (iv), and maximality in all other cases but the third case of (iv). Note that in (iii), $H^1(K_v, E(\overline{K}_v)[\eta])$ equals the unramified subgroup, as its cardinality is ℓ. To get the maximal unramifiedness in the third part of (iv) use Corollary 2.2.20. □

We finish with the main theorem of this section. Recall, that we call $\operatorname{coker} \eta_p$ *maximal* if it equals $H^1(\mathbb{Q}_p, E(\overline{\mathbb{Q}}_p)[\eta])$, and *maximally unramified* if it equals $H^1_{\mathrm{nr}}(\mathbb{Q}_p, E(\overline{\mathbb{Q}}_p)[\eta])$; see the discussion before Remark 2.2.4. The definition of $|\eta'(0)|_p$ is given before Proposition 2.2.13. If $E(\overline{\mathbb{Q}}_p)[\eta] = E(\mathbb{Q}_p)[\eta]$, then we say that η has a $\mathbb{Q}_p$-kernel.

Theorem 2.3.7 (Criteria to classify $\operatorname{coker} \eta_p$ is case η has a $\mathbb{Q}_p$-kernel and is of prime degree)**.** *Let E and E' be elliptic curves over $\mathbb{Q}_p$ and let $\eta : E \to E'$ be an isogeny of prime degree ℓ, and assume that η has a $\mathbb{Q}_p$-kernel. Then the left column of the table below implies the two columns to the right and in all but the last row we also get that $|\eta'(0)|_p = 1$.*

reduction type of $E/\mathbb{Q}_p$, plus further assumptions	$p = $ *or* $\neq \ell$, $\boldsymbol{\mu}_\ell \subseteq$ *or* $\not\subseteq \mathbb{Q}_p$	$\operatorname{coker} \eta_p$ *is*
split multiplicative, $\ker \eta_p \not\subseteq E_0(\overline{\mathbb{Q}}_p)$	*no implications*	*trivial*
split multipl., $\ker \eta_p \subseteq E_0(\overline{\mathbb{Q}}_p)$, $p \neq 2$ *or* $\ell \neq 2$	$p \neq \ell, \boldsymbol{\mu}_\ell \subseteq \mathbb{Q}_p$	*maximal*
non-split multiplicative, $\ell \neq 2$	$p \neq \ell, \boldsymbol{\mu}_\ell \not\subseteq \mathbb{Q}_p$	*max. unramified*
non-split multiplicative, $\ell = 2 \neq p$, $c_{E'}/c_E = 1/2$	$p \neq \ell, \boldsymbol{\mu}_\ell \subseteq \mathbb{Q}_p$	*trivial*
non-split multiplicative, $\ell = 2 \neq p$, $c_{E'}/c_E = 2$	$p \neq \ell, \boldsymbol{\mu}_\ell \subseteq \mathbb{Q}_p$	*maximal*
non-split multiplicative, $\ell = 2 \neq p$, $c_E = c_{E'} = 1$	$p \neq \ell, \boldsymbol{\mu}_\ell \subseteq \mathbb{Q}_p$	*max. unramified*
good, $p \neq 2$ *or* $\ell \neq 2$	*no implications*	*max. unramified*
additive, $\ell \geq 5$, $\lvert\eta'(0)\rvert_p = 1$	$p = \ell, \boldsymbol{\mu}_\ell \not\subseteq \mathbb{Q}_p$	*max. unramified*
additive, $\ell \geq 5$, $\lvert\eta'(0)\rvert_p \neq 1$	$p = \ell, \boldsymbol{\mu}_\ell \not\subseteq \mathbb{Q}_p$	*maximal*

Proof. For all but the first row of the table, we use Lemma 2.2.16 to deduce that η_p^1 is injective. The six cases of multiplicative reduction are contained in the last corollary and the case of good reduction is covered by Lemma 2.2.12.

In the additive case, due to $\ell \geq 5$, we get $p = \ell$, by Lemma 2.3.5, and hence $\boldsymbol{\mu}_\ell \not\subseteq \mathbb{Q}_p$. This implies that $\#H^1(\mathbb{Q}_p, E(\overline{\mathbb{Q}}_p)[\eta]) = \ell^2$, by Corollary 2.2.3. Further $\overline{\eta}_p$ is an isomorphism, by Lemma 2.3.1, and thus by Corollary 2.2.14, we have $\#\operatorname{coker} = \ell \cdot |\eta'(0)|_p^{-1}$. We know that $|\eta'(0)|_p^{-1} \geq 1$ as η_p^1 is injective. Hence, there are two possibilities. Firstly, $\#\operatorname{coker} \eta_p = \ell$, which is equivalent to $|\eta'(0)|_p = 1$, and secondly, $\#\operatorname{coker} \eta_p = \ell^2$, which is equivalent to $|\eta'(0)|_p \neq 1$, and which implies that $\operatorname{coker} \eta_p$ is maximal. It remains to show that $\operatorname{coker} \eta_p$ is maximally unramified in case the reduction type is additive and $|\eta'(0)|_p = 1$. At this point, we apply our main Theorem 2.2.19. All conditions are fulfilled due to Lemma 2.2.16. This finishes the proof. □

2.4. Non-simple abelian varieties and isogenies with diagonal kernel

In this section we present in Setting 2.4.12 the construction of the non-simple abelian surfaces studied throughout the next two chapters. Further, we give the Key Lemma 2.4.5 to control the local quotient with respect to isogenies with diagonal kernel. By K we denote a field of characteristic 0. An abelian variety B/K is called *non-simple* if it is isogenous to a product of two abelian varieties A_1/K and A_2/K:

$$\varphi : A_1 \times A_2 \to B.$$

Recall, that if we do not specify the field of definition of an isogeny φ between two abelian varieties which are defined over a field K, then we want φ to be defined over K, as well. Let A_1, A_2 and B be abelian varieties over a field K and let $\varphi : A_1 \times A_2 \to B$ be an isogeny. We say that φ has *diagonal kernel*, or simply that φ is *diagonal*, if there is a finite group scheme G over K contained in both A_i, together with fixed embeddings $\iota_i : G \hookrightarrow A_i$, such that the kernel of φ is the natural embedding of G into the product $A_1 \times A_2$ via $\iota_1 \times \iota_2$. We denote the image of G in A_i by $G_i := \iota_i(G)$. Clearly, G, G_1 and G_2 are pairwise isomorphic as finite group schemes and the $\overline{K}$-rational points of G_1 and G_2 form isomorphic Galois modules. Hence, there is a Galois equivariant isomorphism $\alpha : G_1 \to G_2$, such that $\iota_2 = \alpha \circ \iota_1$ and $\ker \varphi$ equals the graph of α. Further, both A_i possess an isogeny $\eta_i : A_i \to A_i'$ which is defined through its kernel by setting $\ker \eta_i := G_i$ and $A_i' := A_i/G_i$. Clearly $\ker \eta_1 \cong \ker \eta_2 \cong \ker \varphi$.

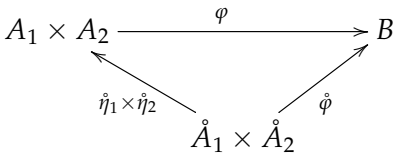
In the next proposition, we show that every isogeny $\varphi : A_1 \times A_2 \to B$ factors as a diagonal isogeny together with a product isogeny. First we present a characterisation of diagonal isogenies.

Lemma 2.4.1. *Let A_1, A_2 and B be abelian varieties over a field K and let $\varphi : A_1 \times A_2 \to B$ be an isogeny. The isogeny φ has diagonal kernel if and only if for all points $(P_1, P_2) \in \ker \varphi_{\overline{K}}$ we have that P_1 is trivial if and only if P_2 is trivial.*

Proof. Assume that φ has diagonal kernel. For a point $(P_1, P_2) \in \ker \varphi_{\overline{K}}$, we have that $P_2 = \alpha(P_1)$, for the Galois equivariant isomorphism $\alpha : G_1 \to G_2$. Hence P_1 is trivial if and only P_2 is trivial.

To prove the other direction, pick two points $(P_1, P_2), (Q_1, Q_2) \in \ker \varphi_{\overline{K}}$. As $(P_1 - Q_1 , P_2 - Q_2) \in \ker \varphi_{\overline{K}}$, we immediately get that $P_1 = Q_1$ if and only if $P_2 = Q_2$. Thus, $\ker \varphi_{\overline{K}}$ determines a set-theoretic bijection $\alpha : G_1 \to G_2$ and it is obvious that $\ker \varphi_{\overline{K}}$ equals the graph of α. It remains to show that α is a Galois equivariant isomorphism. If $(P_1, \alpha(P_1)), (Q_1, \alpha(Q_1)) \in \ker \varphi_{\overline{K}}$, then $(P_1 + Q_1, \alpha(P_1) + \alpha(Q_2)) \in \ker \varphi_{\overline{K}}$, thus $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(Q_2)$, showing that α is a group isomorphism. Finally, $(P_1, \alpha(P_1))^\sigma = (P_1^\sigma, (\alpha(P_1))^\sigma)$ and therefore $\alpha(P_1^\sigma) = (\alpha(P_1))^\sigma$. Thus, α respects the action of Galois. □

Proposition 2.4.2. *Let $\mathring{A}_1, \mathring{A}_2$ and B be abelian varieties over K and let $\mathring{\varphi} : \mathring{A}_1 \times \mathring{A}_2 \to B$ be an isogeny. Then there are two abelian varieties A_1 and A_2 over K together with isogenies $\mathring{\eta}_i : \mathring{A}_i \to A_i$, and there is an isogeny $\varphi : A_1 \times A_2 \to B$ having diagonal kernel, such that the following diagram commutes.*



Proof. Denote the intersection of $\ker \mathring{\varphi}_{\overline{K}}$ with $\mathring{A}_1(\overline{K}) \times \{\mathcal{O}\}$, respectively $\{\mathcal{O}\} \times \mathring{A}_2(\overline{K})$, by $\mathring{G}_1$, respectively $\mathring{G}_2$. As $\mathring{G}_i$ is a Galois invariant subgroup of $\mathring{A}_i(\overline{K})$ we get isogenies $\mathring{\eta}_i : \mathring{A}_i \to A_i := \mathring{A}_i / \mathring{G}_i$. Further, $\mathring{G}_1 \times \mathring{G}_2$ is a Galois invariant subgroup of $\ker \mathring{\varphi}_{\overline{K}}$, thus there is an isogeny $\varphi : A_1 \times A_2 \to B$ such that $\mathring{\varphi} = \varphi \circ (\mathring{\eta}_1 \times \mathring{\eta}_2)$. It remains to show that φ has diagonal kernel.

Fix $(Q_1, Q_2) \in \ker \varphi_{\overline{K}}$. By the previous lemma, we have to show that Q_1 is trivial in $A_1(\overline{K})$ if and only if Q_2 is trivial in $A_2(\overline{K})$. Let $(P_1, P_2) \in \ker \mathring{\varphi}_{\overline{K}}$ be a preimage of (Q_1, Q_2) under $\mathring{\eta}_1 \times \mathring{\eta}_2$. We have to show that $P_1 \in \mathring{G}_1$ if and only if $P_2 \in \mathring{G}_2$. Assume that $P_1 \in \mathring{G}_1$. Then $(P_1, \mathcal{O}) \in \ker \mathring{\varphi}_{\overline{K}}$. Now $(P_1, P_2) - (P_1, \mathcal{O}) = (\mathcal{O}, P_2)$ is also in $\ker \mathring{\varphi}_{\overline{K}}$, and thus $P_2 \in \mathring{G}_2$. In the same manner one shows that if $P_2 \in \mathring{G}_2$ then $P_1 \in \mathring{G}_1$ and the proposition is proven. □

Remark 2.4.3. If B/K is a non-simple abelian surface, then by the previous proposition, there are elliptic curves E_1/K and E_2/K and an isogeny $\varphi : E_1 \times E_2 \to B$ having diagonal kernel. Recall, that product of elliptic curves over number fields have square order Tate-Shafarevich group. Hence, to determine the possible non-square parts of the order of Tate-Shafarevich groups of non-simple abelian surfaces B/K over a number field K, it is sufficient to study isogenies $\varphi : E_1 \times E_2 \to B$ with diagonal kernel, with E_1 and E_2 being elliptic curves over K.

Now we present our Key Lemma to controll the local quotient for isogenies with diagonal kernel. First, we state a basic lemma about Galois cohomology.

Lemma 2.4.4. *Let K be a field and let G_1 and G_2 be two finite K-Galois modules. Assume $\alpha : G_1 \to G_2$ is a Galois equivariant homomorphism. Then the map*

$$\alpha^* : H^1(K, G_1) \to H^1(K, G_2), \ \ [\xi] \mapsto [\alpha \circ \xi],$$

is a well-defined group homomorphism. If in addition α is an isomorphism, then so too is α^* an isomorphism. Further, the isomorphism α^* respects the Inflation-Restriction sequence for normal subgroups of Gal_K, i.e. for any Galois extension L/K, α^* induces an isomorphism $H^1(\mathrm{Gal}(L/K), G_1^{\mathrm{Gal}_L}) \to H^1(\mathrm{Gal}(L/K), G_2^{\mathrm{Gal}_L})$ and an isomorphism $H^1(L, G_1) \to H^1(L, G_2)$ and these isomorphisms commute with the Inflation-Restriction sequence.

In particular, if $K = K_v$ is a local field, then for every Galois equivariant isomorphism $\alpha : G_1 \to G_2$, the isomorphism $\alpha^* : H^1(K_v, G_1) \to H^1(K_v, G_2)$ induces an isomorphism between the unramified subgroups $H^1_{\mathrm{nr}}(K_v, G_1)$ and $H^1_{\mathrm{nr}}(K_v, G_2)$.

Proof. Everything follows directly from the functoriality of Galois cohomology. □

Lemma 2.4.5 (Key Lemma to compute the local quotient for isogenies with diagonal kernel)**.** *Let A_1 and A_2 be two abelian varieties over a number field K and let $\varphi : A_1 \times A_2 \to B$ be an isogeny with diagonal kernel. Denote by $\eta_i : A_i \to A_i'$ the isogenies for which there is a Galois equivariant isomorphism $\alpha : \ker \eta_1 \to \ker \eta_2$ whose graph equals $\ker \varphi$. Let $v \in M_K^0$ be a finite place of K. The following statements hold.*

(i) $\operatorname{coker} \varphi_v$ *is maximal if and only if* $\operatorname{coker} \eta_{1,v}$ *and* $\operatorname{coker} \eta_{2,v}$ *are both maximal.*

(ii) $\operatorname{coker} \varphi_v$ *is trivial if either* $\operatorname{coker} \eta_{1,v}$ *or* $\operatorname{coker} \eta_{2,v}$ *is trivial.*

(iii) $\operatorname{coker} \varphi_v$ *is maximally unramified if either* $\operatorname{coker} \eta_{1,v}$ *or* $\operatorname{coker} \eta_{2,v}$ *is maximally unramified and the other one is maximally unramified or maximal.*

Proof. Define the two Galois equivariant isomorphisms $\gamma_1 := (id, \alpha) : \ker \eta_1 \to \ker \varphi$ and $\gamma_2 := (\alpha^{-1}, id) : \ker \eta_2 \to \ker \varphi$. By the above lemma, we get two group isomorphisms $\gamma_i^* : H^1(K_v, A_i[\eta_i]) \to H^1(K_v, (A_1 \times A_2)[\varphi])$. Thus, for any $[\xi] \in H^1(K_v, (A_1 \times A_2)[\varphi])$ there is a unique $[\xi_1] \in H^1(K_v, A_1[\eta_1])$ and a unique $[\xi_2] \in H^1(K_v, A_2[\eta_2])$ such that $\gamma_1^*([\xi_1]) = \gamma_2^*([\xi_2]) = [\xi]$. It follows that $\xi(\sigma) = (\xi_1(\sigma), \alpha(\xi_1(\sigma)))$ and $\xi(\sigma) = (\alpha^{-1}(\xi_2(\sigma)), \xi_2(\sigma))$, and hence $\xi(\sigma) = (\xi_1(\sigma), \xi_2(\sigma))$, for all $\sigma \in \mathrm{Gal}_{K_v}$. Thus

$$[\xi] \in \operatorname{coker} \varphi_v \ \Leftrightarrow \ [\xi_1] \in \operatorname{coker} \eta_{1,v} \text{ and } [\xi_2] \in \operatorname{coker} \eta_{2,v}, \tag{2.5}$$

since both assertions are equivalent to the existence of $P_1 \in A_1(\overline{K}_v)$ and $P_2 \in A_2(\overline{K}_v)$, such that for all $\sigma \in \mathrm{Gal}_{K_v}$ we have $\xi_1(\sigma) = P_1^\sigma - P_1$ and $\xi_2(\sigma) = P_2^\sigma - P_2$. For part (ii), recall that $[\xi]$ is the trivial class if and only if $[\xi_1]$ and $[\xi_2]$ are both the trivial class. For part (iii), use the above lemma again to get that $[\xi] \in H^1_{\mathrm{nr}}(K_v, (A_1 \times A_2)[\varphi])$ if and only if $[\xi_1] \in H^1_{\mathrm{nr}}(K_v, A_1[\eta_1])$ and $[\xi_2] \in H^1_{\mathrm{nr}}(K_v, A_2[\eta_2])$. Now the lemma follows directly from statement (2.5). □

Remark 2.4.6. The Key Lemma shows that if one knows that $\operatorname{coker} \eta_{1,v}$ and $\operatorname{coker} \eta_{2,v}$ are maximal, maximally unramified, or trivial, then one knows that $\operatorname{coker} \varphi_v$ is maximal, maximally unramified, or trivial. As seen in Section 2.2, knowing these properties

about coker φ_v is sufficient to deduce the quotient $\#\operatorname{coker}\varphi_v/\#\ker\varphi_v$. Hence, combining Theorem 2.3.7, which classifies coker $\eta_{i,p}$, with the Key Lemma, it is possible to compute the local quotient for many cyclic isogenies $\varphi : E_1/\mathbb{Q} \times E_2/\mathbb{Q} \to B/\mathbb{Q}$.

We say that A_1 *and* A_2 *are abelian varieties over* K *having isogenies with isomorphic kernels*, if A_1 and A_2 both possess an isogeny, such that the kernels of these isogenies, which we denote by G_1 and G_2, are isomorphic as finite group schemes. Hence, the $\overline{K}$-rational points of G_1 and G_2 are isomorphic as Galois modules and there is a Galois equivariant isomorphism $\alpha : G_1 \to G_2$. In this case, we can define an isogeny $\varphi : A_1 \times A_2 \to B$ with diagonal kernel by setting the kernel of φ to be equal to the graph of α. Note that φ and B depend on the choice of α, which we may denote by φ_α and B_α to emphasise it. For fixed abelian varieties A_1/K and A_2/K and fixed isomorphic finite subgroup schemes $G_1/K \subset A_1$ and $G_2/K \subset A_2$, we determine conditions under which the size of $Ш(B_\alpha/K)$ is independent of the choice of $\alpha : G_1 \to G_2$. It follows immediately that the order of $Ш(B_\alpha/K)$ is independent of α if φ is a cyclic isogeny. In the rest of this chapter and also in the two subsequent ones, we focus on cyclic isogenies. In Section 5.3, we continue studying conditions under which the order of $Ш(B_\alpha/K)$ is independent of the choice of α for non-cyclic isogenies φ.

Proposition 2.4.7 (Criterion for the independence of $\#Ш(B_\alpha/K)$ with respect to α)**.** *Let A_1 and A_2 be two abelian varieties over a number field K such that there are isomorphic finite K-subgroup schemes $G_1 \subseteq A_1$ and $G_2 \subseteq A_2$. Choose a Galois equivariant isomorphism $\alpha : G_1 \to G_2$ and let $\varphi_\alpha : A_1 \times A_2 \to B_\alpha$ be the isogeny with diagonal kernel such that* $\ker\varphi_\alpha$ *equals the graph of α. If for either $i = 1$ or $i = 2$ all Galois equivariant automorphisms of G_i are induced by endomorphisms of A_i, then $\#Ш(B_\alpha/K)$ is independent of the choice of α.*

Proof. We show that the cardinality of all occurring kernels and cokernels in the local and global quotient of the Cassels-Tate equation (2.1) are independent of α. The set of $\overline{K}$-rational points of the kernels of the isogenies $\varphi_\alpha : A_1 \times A_2 \to B_\alpha$ and $\varphi_\alpha^\vee : B_\alpha^\vee \to A_1^\vee \times A_2^\vee$ depend on α. But the isomorphism class of $\ker\varphi_\alpha$ and of $\ker\varphi_\alpha^\vee$ as a Galois module is fixed, hence it is clear that the size of all occurring kernels in the Cassels-Tate equation are unaffected by α. It remains to consider the cokernels.

Fix two Galois equivariant isomorphisms $\alpha : G_1 \to G_2$ and $\alpha' : G_1 \to G_2$. Then there are Galois equivariant automorphisms β_1 of G_1 and β_2 of G_2 such that $\alpha = \alpha' \circ \beta_1$ and $\alpha' = \beta_2 \circ \alpha$. The Galois equivariant automorphisms $\gamma_1 := \beta_1 \times id$ and $\gamma_2 := id \times \beta_2$ of $G_1 \times G_2$ induce Galois equivariant isomorphisms between $\ker\varphi_\alpha$ and $\ker\varphi_{\alpha'}$. We consider the case $i = 2$, i.e. we assume that the automorphisms of G_2 are liftable to endomorphisms of A_2. The proof for $i = 1$ works in an analogous way.

Denote a lift of β_2 by B_2. Then the following diagram has exact rows and commutes, with the vertical maps $id \times B_2$ and $[id \times B_2]$ being isogenies.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker\varphi_\alpha & \longrightarrow & A_1 \times A_2 & \xrightarrow{\varphi_\alpha} & B_\alpha & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle id\times B_2} & & \downarrow{\scriptstyle [id\times B_2]} & & \\ 0 & \longrightarrow & \ker\varphi_{\alpha'} & \longrightarrow & A_1 \times A_2 & \xrightarrow{\varphi_{\alpha'}} & B_{\alpha'} & \longrightarrow & 0 \end{array}$$

Applying Galois cohomology yields the following commutative diagram with exact rows, where L denotes either the number field K or one of its completions K_v.

$$\begin{array}{ccccccc}
0 & \longrightarrow & \operatorname{coker}\varphi_{\alpha,L} & \longrightarrow & H^1(L,\ker\varphi_\alpha) & \xrightarrow{\iota^1_\alpha} & H^1(L,A_1\times A_2)\longrightarrow\dots \\
 & & \downarrow & & \downarrow{\scriptstyle\gamma_2^*} & & \downarrow{\scriptstyle(id\times B_2)^*} \\
0 & \longrightarrow & \operatorname{coker}\varphi_{\alpha',L} & \longrightarrow & H^1(L,\ker\varphi_{\alpha'}) & \xrightarrow{\iota^1_{\alpha'}} & H^1(L,A_1\times A_2)\longrightarrow\dots
\end{array}$$

The homomorphism γ_2^* is an isomorphism by Lemma 2.4.4. As the diagram commutes, we get that γ_2^* induces an injection $\ker\iota^1_\alpha \hookrightarrow \ker\iota^1_{\alpha'}$. Switching the roles of α and α', for which we need the liftability of β_2^{-1}, gives an injection $\ker\iota^1_{\alpha'} \hookrightarrow \ker\iota^1_\alpha$. Thus, $\operatorname{coker}\varphi_{\alpha,L}$ and $\operatorname{coker}\varphi_{\alpha',L}$ have same cardinality. Now consider the dual picture, where $\gamma_2^\vee$ is an isomorphism making the following diagram commute.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \ker\varphi^\vee_{\alpha'} & \longrightarrow & B^\vee_{\alpha'} & \xrightarrow{\varphi^\vee_{\alpha'}} & A_1^\vee\times A_2^\vee & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\gamma_2^\vee} & & \downarrow{\scriptstyle[id\times B_2]^\vee} & & \downarrow{\scriptstyle id\times B_2^\vee} & & \\
0 & \longrightarrow & \ker\varphi^\vee_{\alpha} & \longrightarrow & B^\vee_{\alpha} & \xrightarrow{\varphi^\vee_{\alpha}} & A_1^\vee\times A_2^\vee & \longrightarrow & 0
\end{array}$$

With the same argument as before, one gets a bijection between $\operatorname{coker}\varphi^\vee_{\alpha,K}$ and $\operatorname{coker}\varphi^\vee_{\alpha',K}$ and thus they have the same number of elements. This finishes the proof of the proposition. □

In case φ is cyclic, the assumption that all Galois equivariant automorphisms of the G_i are induced by endomorphisms of A_i is automatically fulfilled, as all these automorphisms are induced by multiplication-by-n endomorphisms of A_i.

Corollary 2.4.8. *Let A_1 and A_2 be two abelian varieties over a number field K, such that there are isomorphic finite cyclic K-subgroup schemes $G_1 \subseteq A_1$ and $G_2 \subseteq A_2$. Choose a Galois equivariant isomorphism $\alpha : G_1 \to G_2$ and let $\varphi_\alpha : A_1 \times A_2 \to B_\alpha$ be the cyclic isogeny with diagonal kernel such that* $\ker\varphi_\alpha$ *equals the graph of α. Then $\#Ш(B_\alpha/K)$ is independent of the choice of α.*

Proof. This follows directly from Proposition 2.4.7 and the comment above. □

If A_1 and A_2 are isogenous by an isogeny Φ which induces the Galois equivariant isomorphism $\alpha : G_1 \to G_2$, then we know a lot about the structure of B. This is shown in the next lemma, proposition, and corollary.

Lemma 2.4.9. *Let A_1 and A_2 be two abelian varieties over a field K and let $\varphi : A_1 \times A_2 \to B$ be an isogeny with diagonal kernel. Let $\alpha : G_1 \to G_2$ be the Galois equivariant isomorphism such that* $\ker\varphi$ *equals the graph of α. As usual we have the isogenies $\eta_i : A_i \to A_i' := A_i/G_i$.*

(i) Assume there is an isogeny $\Phi : A_1 \to A_2$, such that $\alpha(P) = \Phi(P)$, for all P in $G_1(\overline{K})$. Then B is isomorphic to $A_1' \times A_2$.

(ii) Assume there is an isogeny $\Phi : A_2 \to A_1$, such that $\alpha^{-1}(P) = \Phi(P)$, for all P in $G_2(\overline{K})$. Then B is isomorphic to $A_1 \times A_2'$.

Proof. We only prove (i). The proof for (ii) works in a similar way. Define two isogenies $\psi_1 : A_1 \times A_1 \to B$ and $\psi_2 : A_1 \times A_1 \to A_1' \times A_2$, by setting

$$\psi_1(P,Q) := \varphi(P, \Phi(Q)), \;\; \psi_2(P,Q) := (\eta_1(P), \Phi(P-Q)).$$

On $\overline{K}$-rational points the kernel of ψ_1 consists of pairs (P,Q), such that P is in the kernel of η_1 and $\alpha(P) = \Phi(Q)$. The kernel of ψ_2 consists of pairs (P,Q), such that P is in the kernel of η_1 and $\Phi(P) = \Phi(Q)$. Therefore, the kernels of ψ_1 and ψ_2 agree if $\alpha(P) = \Phi(P)$, for all P in $G_1(\overline{K})$. □

In case the degrees of φ and Φ are coprime, we get the following statement.

Proposition 2.4.10. *Let A_1 and A_2 be two abelian varieties over a field K and let $\varphi : A_1 \times A_2 \to B$ be an isogeny with diagonal kernel. Assume A_1 and A_2 are isogenous by an isogeny Φ of degree coprime to the degree of φ.*

(i) If all Galois equivariant automorphisms of G_1 are induced by endomorphisms of A_1, then B is isomorphic to $A_1 \times A_2'$.

(ii) If all Galois equivariant automorphisms of G_2 are induced by endomorphisms of A_2, then B is isomorphic to $A_1' \times A_2$.

Proof. Let φ be defined with respect to $\alpha : G_1 \to G_2$. We only show (ii), as (i) can be shown in an analogous way. Assume w.l.o.g. that Φ is an isogeny from A_1 to A_2. As seen in the previous lemma, we have to show that there is an isogeny $\Phi' : A_1 \to A_2$, such that $\alpha(P) = \Phi'(P)$, for all P in G_1. Since the degree of Φ and φ is coprime, Φ induces a Galois equivariant isomorphism between G_1 and G_2, hence there is an automorphism β_2 of G_2 such that $\alpha(P) = \beta_2(\Phi(P))$, for all P in G_1. Let β_2 be induced by the endomorphism B_2 of A_2. Define the isogeny $\Phi' := B_2 \circ \Phi : A_1 \to A_2$. It is easy to see that $\alpha(P) = \Phi'(P)$, for all P in G_1, as $\alpha(P) = \beta_2(\Phi(P)) = B_2(\Phi(P)) = \Phi'(P)$, hence we are done. □

As already mentioned in Corollary 2.4.8, in case the isogeny $\varphi : A_1 \times A_2 \to B$ is cyclic, then all automorphisms of the G_i are liftable to endomorphisms of A_i.

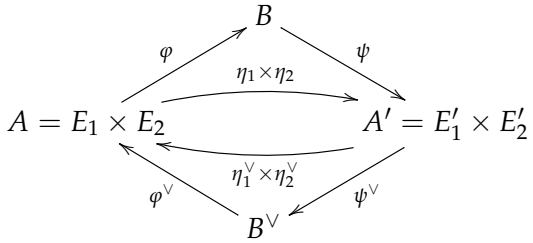
Corollary 2.4.11. *Let A_1 and A_2 be abelian varieties over a field K and let $\varphi : A_1 \times A_2 \to B$ be a cyclic isogeny with diagonal kernel. If further A_1 and A_2 are isogenous by an isogeny of degree coprime to the degree of φ, then B is isomorphic to $A_1' \times A_2$ and to $A_1 \times A_2'$.*

Proof. This follows directly from Proposition 2.4.10 and the comment above. □

Now we have a look at the special case of A_1 and A_2 being elliptic curves E_1 and E_2 over $\mathbb{Q}$, i.e. we focus on non-simple abelian surfaces $B/\mathbb{Q}$. The following setting is used in the remainder of this chapter and throughout the next two chapters.

Setting 2.4.12. Let N be a positive integer and let E_1 and E_2 be two elliptic curves over $\mathbb{Q}$, each having a $\mathbb{Q}$-rational point P_i of exact order N. The point P_i generates a finite subgroup scheme $G_i := \langle P_i \rangle$ in E_i. Denote by $E_i' := E_i/G_i$ the quotient and by $\eta_i : E_i \to E_i'$ the corresponding quotient isogeny. Set $A := E_1 \times E_2$ to be the product and define in A the finite subgroup scheme $\tilde{G} := \langle (P_1, nP_2) \rangle$, for

some $n \in (\mathbb{Z}/N\mathbb{Z})^*$. Define $B := A/\tilde{G}$ to be the quotient and denote the corresponding isogeny by $\varphi : A \to B$. Hence, φ is a cyclic isogeny with diagonal kernel of degree N. Further, φ has a $\mathbb{Q}$-kernel and thus φ_p has a $\mathbb{Q}_p$-kernel for every place p of $\mathbb{Q}$. Now set $A' := E_1' \times E_2'$ and denote by $\eta_1 \times \eta_2 : E_1 \times E_2 \to E_1' \times E_2'$ the isogeny having as kernel $G_1 \times G_2$. We let $\psi : B \to A'$ be the isogeny satisfying $\eta_1 \times \eta_2 = \psi \circ \varphi$. Note that, as elliptic curves are principally polarised, we have $A \cong A^\vee$ and $A' \cong A'^\vee$. To summarise, we have a commutative diagram:



By construction, $\ker \eta_1 \cong \ker \eta_2 \cong \ker \varphi \cong \mathbb{Z}/N\mathbb{Z}$, hence $\ker(\eta_1 \times \eta_2) \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ and $\ker \psi \cong \mathbb{Z}/N\mathbb{Z}$. Since the kernels of the dual isogenies are the Cartier duals, we have $\ker \eta_1^\vee \cong \ker \eta_2^\vee \cong \ker \varphi^\vee \cong \ker \psi^\vee \cong \boldsymbol{\mu}_N$ and $\ker(\eta_1^\vee \times \eta_2^\vee) \cong \boldsymbol{\mu}_N \times \boldsymbol{\mu}_N$.

Remark 2.4.13. (i) Let G be a finite group scheme which is isomorphic to the group schemes G_1 and G_2, i.e. $G \cong \mathbb{Z}/N\mathbb{Z}$. Fix a generating point P, i.e. $G = \langle P \rangle$. Then there are natural embeddings ι_i of G into E_i with image G_i given by $\iota_1(P) := P_1$ and $\iota_2(P) := nP_2$, such that $\tilde{G}$ is the embedding of G into A with respect to $\iota_1 \times \iota_2$. The Galois equivariant isomorphism $\alpha : G_1 \to G_2$ fulfilling the condition $\iota_2 = \alpha \circ \iota_1$ is defined by $P_1 \mapsto nP_2$. In other words, the choice of n is equivalent to the choice of α. As we have seen in Corollary 2.4.8, the order of $Ш(B/\mathbb{Q})$ is independent of that choice.

(ii) Due to Mazur's classification of possible torsion points of elliptic curves over $\mathbb{Q}$, Theorem 7.5 in [Sil86] or [Maz77b] and [Maz78], the only possible values for N in Setting 2.4.12 are $N = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$.

(iii) If $\#Ш(B/\mathbb{Q}) = k \cdot \square$, with k square-free, then k has to divide N. Thus, the only possible values for k that one can obtain with Setting 2.4.12 are $k = 1, 2, 3, 5, 6, 7, 10$. In the next chapter, we show that indeed all these values for k are possible.

The next lemma tells us that the abelian surface $B/\mathbb{Q}$ from Setting 2.4.12 has the interesting property that every polarisation it possesses has degree divisible by ℓ, in case $\deg \varphi = N = \ell$ is a prime and E_1 and E_2 are not isogenous. The proof we present follows a sketch of Brian Conrad.

Lemma 2.4.14. *Let K be a field and let E_1 and E_2 be two non-isogenous elliptic curves over K. Let G be a finite cyclic group scheme of prime order ℓ over K together with fixed embeddings $\iota_1 : G \hookrightarrow E_1$ and $\iota_2 : G \hookrightarrow E_2$. Thus the map $\iota_1 \times \iota_2$ is a diagonal embedding of G into the product $A := E_1 \times E_2$. Denote its image in A by $\tilde{G}$. Then any polarisation of the quotient $B := A/\tilde{G}$ has degree divisible by ℓ.*

Proof. Let $\lambda : B \to B^\vee$ be any polarisation and consider the quotient map $\varphi : A \to B$ and its dual $\varphi^\vee : B^\vee \to A^\vee = A$. The composition

$$\Psi : A \xrightarrow{\varphi} B \xrightarrow{\lambda} B^\vee \xrightarrow{\varphi^\vee} A$$

is a polarisation of A. Denote by $\mathrm{em}_i : E_i \hookrightarrow A$ the natural embedding of E_i into the product, and by $\mathrm{pr}_i : A \to E_i$ the natural projection. Define homomorphisms

$$\Psi_1 : E_1 \xrightarrow{\mathrm{em}_1} A \xrightarrow{\Psi} A \xrightarrow{\mathrm{pr}_1} E_1 \quad \text{and} \quad \Psi_2 : E_2 \xrightarrow{\mathrm{em}_2} A \xrightarrow{\Psi} A \xrightarrow{\mathrm{pr}_2} E_2.$$

We claim that $\Psi = \Psi_1 \times \Psi_2$. The claim is equivalent to $\mathrm{pr}_2 \circ \Psi \circ \mathrm{em}_1 : E_1 \to E_2$ and $\mathrm{pr}_1 \circ \Psi \circ \mathrm{em}_2 : E_2 \to E_1$ being the zero maps. By assumption, E_1 and E_2 are non-isogenous, hence all homomorphism between them are the zero map, giving the claim.

It follows that for $i = 1$ and $i = 2$ we get that Ψ_i is a polarisation of E_i having $\iota_i(G)$ in its kernel. As the degree of a polarisation is always a square and ℓ is a prime we get that ℓ^2 divides the degree of Ψ_1 and of Ψ_2. Therefore, ℓ^4 divides the degree of Ψ. We conclude that ℓ^2 divides the degree of the polarisation λ, as $\deg \Psi = \deg \varphi \cdot \deg \lambda \cdot \deg \varphi^\vee = \ell^2 \cdot \deg \lambda$, which completes the proof. □

In the next remark we show that it is enough to be able to compute the Cassels-Tate equation for isogenies of prime power degree. This enables us to deal with Setting 2.4.12 for the composite cases $N = 6$ and $N = 10$. Further, it has a nice implication in case we consider cyclic isogenies $\varphi : E_1 \times E_2 \to B$ with diagonal kernel for E_1 and E_2 being isogenous elliptic curves, as shown in the corollary thereafter.

Remark 2.4.15. Let A and B be abelian varieties over a field K and let $\varphi : A \to B$ be an isogeny. Denote by $\prod_i \ell_i^{e_i}$ the prime factorisation of $\deg \varphi$, with the ℓ_i being pairwise different primes. The ℓ_i-primary part of the $\overline{K}$-rational points of $\ker \varphi$ forms a Galois invariant subgroup. Hence for each ℓ_i, φ factors through an isogeny $\varphi_{\ell_i} : A \to B_{\ell_i}$ of degree $\ell_i^{e_i}$ by defining $\ker \varphi_{\ell_i}$ to be the subgroup scheme of $\ker \varphi$ of order $\ell_i^{e_i}$. Therefore, there is an isogeny $\psi_{\ell_i} : B_{\ell_i} \to B$ of degree coprime to ℓ_i, such that $\varphi = \psi_{\ell_i} \circ \varphi_{\ell_i}$. Thus, the ℓ_i-primary parts of $Ш(B_{\ell_i}/K)$ and $Ш(B/K)$ are isomorphic. For the dual isogeny, we get an analogous decomposition $\varphi^\vee = \psi_{\ell_i}^\vee \circ \varphi_{\ell_i}^\vee$. Note that $\varphi_{\ell_i}^\vee := (\varphi^\vee)_{\ell_i} \neq (\varphi_{\ell_i})^\vee$. Now let K be a number field. Hence, in order to compute the Cassels-Tate equation (2.1) for φ it suffices to compute all the Cassels-Tate equations for the φ_{ℓ_i}. As the degrees of all φ_{ℓ_i} are pairwise coprime we get

$$\operatorname{coker} \varphi_K = \prod_i \operatorname{coker} \varphi_{\ell_i,K}, \ \operatorname{coker} \varphi_K^\vee = \prod_i \operatorname{coker} \varphi_{\ell_i,K}^\vee, \ \operatorname{coker} \varphi_v = \prod_i \operatorname{coker} \varphi_{\ell_i,v}.$$

The same is true for the kernels and hence we compute

$$\frac{\#\ker \varphi_K}{\#\operatorname{coker} \varphi_K} = \prod_i \frac{\#\ker \varphi_{\ell_i,K}}{\#\operatorname{coker} \varphi_{\ell_i,K}}, \ \frac{\#\operatorname{coker} \varphi_K^\vee}{\#\ker \varphi_K^\vee} = \prod_i \frac{\#\operatorname{coker} \varphi_{\ell_i,K}^\vee}{\#\ker \varphi_{\ell_i,K}^\vee}, \ \frac{\#\operatorname{coker} \varphi_v}{\#\ker \varphi_v} = \prod_i \frac{\#\operatorname{coker} \varphi_{\ell_i,v}}{\#\ker \varphi_{\ell_i,v}}.$$

In case $\varphi : A_1 \times A_2 \to B$ has diagonal kernel then all the φ_{ℓ_i} also have diagonal kernel.

Corollary 2.4.16. *Let E_1 and E_2 be two elliptic curves over a number field K and let $\varphi : E_1 \times E_2 \to B$ be a cyclic isogeny with diagonal kernel of degree N. Assume E_1 and E_2 are isogenous by a degree M isogeny.*

(i) If $\gcd(N, M) = 1$, e.g. E_1 and E_2 are isomorphic, then B/K is isomorphic to the product of two elliptic curves and therefore $\#Ш(B/K) = \square$.

(ii) Let k be a square-free positive integer, such that $\#Ш(B/K) = k \cdot \square$. If a prime ℓ divides k, then ℓ divides $\gcd(N, M)$.

Proof. The first part follows directly from Corollary 2.4.11 and the fact that the Tate-Shafarevich group of $E_1 \times E_2$ has square order.

For (ii) write $N = \prod_i \ell_i^{e_i}$, with ℓ_i pairwise different primes. Thus we get the cyclic isogenies $\varphi_{\ell_i} : E_1 \times E_2 \to B_{\ell_i}$ with diagonal kernel of degree $\ell_i^{e_i}$. If $\ell \mid k$, then clearly $\ell = \ell_i$, for some i. Hence, $\ell \mid N$. Further, $\ell_i \mid k$ if and only if $\#Ш(B_{\ell_i}/K) = \ell_i \cdot \square$. By (i), it follows that $\#Ш(B_{\ell_i}/K) = \square$, for $\ell_i \nmid M$, which completes the proof. □

We end this chapter with a general lemma about the torsion and global quotient of the Cassels-Tate equation (2.1) for an isogeny $\varphi : A_1 \times A_2 \to B$ with diagonal kernel. The lemma is not needed before Chapter 5, but is uses the notation we established in this section. Recall, that if an abelian variety has Mordell-Weil rank equal to 0, then its regulator equals 1, hence in case both abelian varieties A_1 and A_2 are of rank 0, then the regulator quotient is 1. There is also a simple condition for triviality of the torsion quotient.

Lemma 2.4.17. *Let A_1 and A_2 be abelian varieties over a field K and let $\varphi : A_1 \times A_2 \to B$ be any isogeny with diagonal kernel. Denote by $\eta_i : A_i \to A_i'$ the isogenies with respect to φ, i.e. there is a Galois equivariant isomorphism $\alpha : \ker \eta_1 \to \ker \eta_2$ such that $\ker \varphi$ equals the graph of α. Denote by $\psi : B \to A_1' \times A_2'$ the isogeny, such that $\psi \circ \varphi = \eta_1 \times \eta_2$.*

(i) Assume that the ℓ-primary parts of the K-rational torsion of all four abelian varieties A_1, A_2, A_1' and A_2' are trivial, for all primes ℓ dividing the degree of φ, i.e. $\gcd(\deg \varphi, \#A_1(K)_{\text{tors}}) = \gcd(\deg \varphi, \#A_2(K)_{\text{tors}}) = \gcd(\deg \varphi, \#A_1'(K)_{\text{tors}}) = \gcd(\deg \varphi, \#A_2'(K)_{\text{tors}}) = 1$. Then the torsion quotient for φ equals 1.

(ii) Assume that the Mordell-Weil groups of all four abelian varieties A_1, A_2, A_1' and A_2' are trivial. Then the global quotient for φ equals 1.

Proof. For primes $\ell \nmid \deg \varphi$ the ℓ-primary parts of the K-rational torsion of $A_1 \times A_2$, B, and $B^\vee$ are isomorphic, hence the ℓ-primary part of the torsion quotient equals 1.

For $\ell \mid \deg \varphi$, the triviality of the torsion of the four abelian varieties implies on the one hand that the ℓ-primary parts of the kernels of φ_K and $\psi_K^\vee$ are trivial, and on the other hand that the ℓ-primary parts of the kernels of $\varphi_K^\vee$ and ψ_K equal the ℓ-primary parts of the K-rational torsion of B and $B^\vee$. As $\ker \varphi \cong \ker \psi$ and $\ker \varphi^\vee \cong \ker \psi^\vee$, we deduce that the ℓ-primary parts of the K-rational torsion of B and $B^\vee$ are trivial. Hence, the torsion quotient equals 1, finishing the proof for (i). Part (ii) is immediate from (i) and the comment above. □

3 Chapter 3.

Constructing non-simple abelian surfaces over $\mathbb{Q}$ with non-square order Tate-Shafarevich groups using elliptic curves with a rational N-torsion point

In this chapter, we construct non-simple non-principally polarised abelian surfaces $B/\mathbb{Q}$, such that $\#Ш(B/\mathbb{Q}) = k \cdot \square$, for $k = 1, 2, 3, 5, 6, 7, 10$. All these examples are obtained via an isogeny $\varphi : E_1 \times E_2 \to B$ as constructed in Setting 2.4.12 with respect to $\deg \varphi = N = 5, 6, 7, 10$. The elliptic curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ have a $\mathbb{Q}$-rational N-torsion point, thus they correspond to points on the modular curve $X_1(N)$. The genus of $X_1(N)$ equals 0 if and only if $N = 1, 2, \ldots, 10, 12$. In this case, the set of $\mathbb{Q}$-rational points of $X_1(N)$ is non-empty. Hence, there are infinitely many elliptic curves over $\mathbb{Q}$ possessing a $\mathbb{Q}$-rational point of order N and these curves can be parametrised by a rational number $d \in \mathbb{Q}$. The parametrisations we use is taken from Proposition 1.1.2 of [Klo01] and Section 6 of [KS03], also see Exercise 8.13 and Remark 7.8 of Chapter VIII of [Sil86]. The goal is to express the local and the global quotient of the Cassels-Tate equation (2.1) with respect to such a parametrisation, i.e. with respect to two rational numbers d_1 and d_2, which represent the two elliptic curves E_1 and E_2. Therefore, for a fixed N we look at a two parameter family of abelian surfaces $B/\mathbb{Q}$.

In the first two sections, we compute the local and the global quotient of the Cassels-Tate equation (2.1) with respect to Setting 2.4.12 with a focus on N being a prime number ℓ. We provide a formula which computes the local quotient with respect to the reduction type of E_1 and E_2 at the primes p; see Theorem 3.1.2. Further, we explain how to obtain two functions with which one can compute the global quotient, as long as Mordell-Weil bases for E_1 and E_2 are known.

In the two prime cases, $N = 5$ and $N = 7$, the results of Chapter 2 enable us to give a formula computing the local and the torsion quotient for any given pair of rational numbers (d_1, d_2) that correspond to the two elliptic curves via the chosen parametrisation. Further, we compute the two functions to determine the global quotient once a Mordell-Weil basis of E_1 and E_2 is known. This is discussed in the third section

of this chapter and provides examples of non-simple abelian surfaces B over $\mathbb{Q}$, such that $\#Ш(B/\mathbb{Q}) = k \cdot \square$, for $k = 5, 7$. Since for any given pair (d_1, d_2) we can compute whether $\#Ш(B/\mathbb{Q})$ is five or seven times a square, provided we have the corresponing Mordell-Weil bases, we are able to obtain comprehensive numerical results about the occurrence of non-square order Tate-Shafarevich groups in these two families of abelian surfaces. We did so for $N = 5$ and the results are presented in Chapter 4 of this work.

The final section of this chapter deals with the composite cases $N = 6$ and $N = 10$, and we give examples of non-simple abelian surfaces B over $\mathbb{Q}$, such that $\# Ш(B/\mathbb{Q}) = k \cdot \square$, for $k = 1, 2, 3, 6, 10$.

3.1. The local quotient

We want to compute the quotients $\#\operatorname{coker}\varphi_p/\#\ker\varphi_p$ with respect to Setting 2.4.12. If p is the place at infinity, we denote the induced map on $\mathbb{R}$-rational points by φ_∞. It is often very easy to compute $\#\operatorname{coker}\varphi_\infty/\#\ker\varphi_\infty$.

Lemma 3.1.1. *Let E_1 and E_2 be elliptic curves over $\mathbb{R}$ and $\varphi : E_1 \times E_2 \to B$ a diagonal cyclic isogeny of degree N having a $\mathbb{R}$-kernel, i.e. $\#\ker\varphi_\infty = N$.*

(i) If $2 \nmid N$, then $\operatorname{coker}\varphi_\infty$ is trivial, and thus $\#\operatorname{coker}\varphi_p/\#\ker\varphi_p = 1/N$.

(ii) If $2 \mid N$ assume further that both elliptic curves have negative discriminant. Then $\#\operatorname{coker}\varphi_\infty = 2$, and thus $\#\operatorname{coker}\varphi_p/\#\ker\varphi_p = 2/N$.

Proof. The first part follows directly from Lemma 2.2.23. For (ii) note that by the long exact sequence of Galois cohomology, $\operatorname{coker}\varphi_\infty$ injects into $H^1(\mathbb{R}, (E_1 \times E_2)[\varphi])$. By assumption, the Galois action on the kernel of φ is trivial hence $H^1(\mathbb{R}, (E_1 \times E_2)[\varphi])$ is just the group of homomorphisms from $\mathbb{Z}/2\mathbb{Z}$ to $\mathbb{Z}/N\mathbb{Z}$, which has 2 elements, if $2 \mid N$. In case both discriminants of the two elliptic curves are negative, we have that $H^1(\mathbb{R}, (E_1 \times E_2)(\mathbb{C}))$ is trivial, by Theorem V.2.4 in [Sil86], implying that $\operatorname{coker}\varphi_\infty$ surjects onto $H^1(\mathbb{R}, (E_1 \times E_2)[\varphi])$, hence it consists of two elements. □

Now we state the main theorem about the local quotient with respect to Setting 2.4.12 for $\deg\varphi = N = \ell$ being prime. It expresses $\#\operatorname{coker}\varphi_p/\#\ker\varphi_p$ in terms of the type of reduction of both E_i at p. In case the reduction type is split multiplicative we additionally have to consider whether $\ker\eta_{i,p} \subseteq (E_i)_0(\mathbb{Q}_p)$, and in case the reduction type is non-split multiplicative we also have to consider the value of the Tamagawa quotient $c(E_i')_p/c(E_i)_p$. In case the reduction type is additive, the local quotient also depends on the values of $|\eta_i'(0)|_p$. Further, we have to do some restrictions on p or ℓ. If $\ell \geq 5$, then the theorem determines the size of $\#\operatorname{coker}\varphi_p/\#\ker\varphi_p$ for any p and any combination of reduction types of the two elliptic curves.

Theorem 3.1.2. *Assume Setting 2.4.12 for* $\deg\varphi = N = \ell$ *being prime and let* $p \in M_{\mathbb{Q}}^0$ *be a finite place. Then the local quotient at* p *can be computed as follows in case* $\ell \geq 5$.

$$\frac{\#\operatorname{coker}\varphi_p}{\#\ker\varphi_p} = \begin{cases} 1/\ell, & \text{at least one elliptic curve } E_i \text{ has split multiplicative} \\ & \quad \text{reduction at } p \text{ with } \ker\eta_{i,p} \nsubseteq (E_i)_0(\mathbb{Q}_p) \\ \ell, & \text{both elliptic curves have split multiplicative reduction at } p \\ & \quad \text{and both } \ker\eta_{i,p} \subseteq (E_i)_0(\mathbb{Q}_p) \\ \ell, & \text{both elliptic curves have additive reduction at } p \\ & \quad \text{and both satisfy } |\eta_i'(0)|_p \neq 1 \\ 1, & \text{otherwise.} \end{cases}$$

In case $\ell = 3$ *we get the following equality.*

$$\frac{\#\operatorname{coker}\varphi_p}{\#\ker\varphi_p} = \begin{cases} 1/3, & \text{at least one elliptic curve } E_i \text{ has split multiplicative} \\ & \quad \text{reduction at } p \text{ with } \ker\eta_{i,p} \nsubseteq (E_i)_0(\mathbb{Q}_p) \\ 3, & \text{both elliptic curves have split multiplicative reduction at } p \\ & \quad \text{and both } \ker\eta_{i,p} \subseteq (E_i)_0(\mathbb{Q}_p) \\ 1, & \text{all other cases, such that neither elliptic curve} \\ & \quad \text{has additive reduction at } p. \end{cases}$$

And in case $\ell = 2 \neq p$ *the situation is the following.*

$$\frac{\#\operatorname{coker}\varphi_p}{\#\ker\varphi_p} = \begin{cases} 1/2, & \text{at least one elliptic curve } E_i \text{ has split multiplicative} \\ & \quad \text{reduction at } p \text{ with } \ker\eta_{i,p} \nsubseteq (E_i)_0(\mathbb{Q}_p) \\ 1/2, & \text{at least one elliptic curve } E_i \text{ has non-split multiplicative} \\ & \quad \text{reduction at } p \text{ with } c(E_i')_p/c(E_i)_p = 1/2, \\ 2, & \text{both elliptic curves have either split multiplicative reduction} \\ & \quad \text{at } p \text{ with } \ker\eta_{i,p} \subseteq (E_i)_0(\mathbb{Q}_p) \text{ or non-split multiplicative} \\ & \quad \text{reduction at } p \text{ with } c(E_i')_p/c(E_i)_p = 2, \\ 1, & \text{all other cases, such that neither elliptic curve has} \\ & \quad \text{additive reduction at } p, \text{ and } (c(E_i')_p, c(E_i)_p) \neq (2,2) \\ & \quad \text{in case } E_i \text{ has non-split multiplicative reduction.} \end{cases}$$

In case $\ell = 2 = p$ *we get that* $\#\operatorname{coker}\varphi_p/\#\ker\varphi_p = 1/2$, *if at least one elliptic curve* E_i *has split multiplicative reduction at* p *with* $\ker\eta_{i,p} \nsubseteq (E_i)_0(\mathbb{Q}_p)$.

Proof. Use Theorem 2.3.7 and the Key Lemma 2.4.5 to deduce from the reduction type of both E_i at p plus the stated further conditions whether $\operatorname{coker}\varphi_p$ is maximal, maximally unramified or trivial, i.e. by Corollary 2.2.3 has order ℓ^2, ℓ, or 1 respectively. As $\#\ker\varphi_p = \ell$ we are done. □

Note, it is impossible that one of the elliptic curves has split multiplicative reduction with $\ker \eta_{i,p} \subseteq (E_i)_0(\mathbb{Q}_p)$ and the other curve has additive reduction with $|\eta_i'(0)|_p \neq 1$, as the former case implies $p \neq \ell$ and the latter case implies $p = \ell$.

3.2. The global quotient

Now we investigate the global quotient $\#\ker \varphi_{\mathbb{Q}} / \#\operatorname{coker} \varphi_{\mathbb{Q}} \cdot \#\operatorname{coker} \varphi_{\mathbb{Q}}^\vee / \#\ker \varphi_{\mathbb{Q}}^\vee$ with respect to Setting 2.4.12, for $\deg \varphi = N = \ell$ being prime. As φ has a $\mathbb{Q}$-kernel, we only need a strategy to compute the size of the cokernels. The method we provide to compute the global quotient is based on knowing generators of the cokernels of $\eta_{i,\mathbb{Q}}$ and $\eta_{i,\mathbb{Q}}^\vee$. Clearly, having a Mordell-Weil basis for $E_i(\mathbb{Q})$ and $E_i'(\mathbb{Q})$ is enough to get such generators. The surjectivity of $\ker \eta_{1,\mathbb{Q}}^\vee \times \ker \eta_{2,\mathbb{Q}}^\vee \to \ker \varphi_{\mathbb{Q}}^\vee$ and $\ker \eta_{1,\mathbb{Q}} \times \ker \eta_{2,\mathbb{Q}} \to \ker \psi_{\mathbb{Q}}$ gives two short exact sequences of the cokernels.

$$0 \to \operatorname{coker} \psi_{\mathbb{Q}}^\vee \to \operatorname{coker} \eta_{1,\mathbb{Q}}^\vee \times \operatorname{coker} \eta_{2,\mathbb{Q}}^\vee \to \operatorname{coker} \varphi_{\mathbb{Q}}^\vee \to 0$$

$$0 \to \operatorname{coker} \varphi_{\mathbb{Q}} \to \operatorname{coker} \eta_{1,\mathbb{Q}} \times \operatorname{coker} \eta_{2,\mathbb{Q}} \to \operatorname{coker} \psi_{\mathbb{Q}} \to 0$$

We first compute $\operatorname{coker} \varphi_{\mathbb{Q}}^\vee$, which is simpler than the computation of $\operatorname{coker} \varphi_{\mathbb{Q}}$. We have the following long exact sequences of Galois cohomology.

$$0 \longrightarrow \operatorname{coker} \eta_{1,\mathbb{Q}}^\vee \times \operatorname{coker} \eta_{2,\mathbb{Q}}^\vee \longrightarrow H^1(\mathbb{Q}, (E_1' \times E_2')(\overline{\mathbb{Q}})[\eta_1^\vee \times \eta_2^\vee]) \longrightarrow \dots$$

$$0 \longrightarrow \operatorname{coker} \varphi_{\mathbb{Q}}^\vee \longrightarrow H^1(\mathbb{Q}, B^\vee(\overline{\mathbb{Q}})[\varphi^\vee]) \longrightarrow \dots$$

The Kummer sequence for a number field K and Hilbert's Theorem 90 yield

$$\delta_K : H^1(K, \boldsymbol{\mu}_\ell) \cong K^* / K^{*\ell}.$$

Since $E_i'(\overline{\mathbb{Q}})[\eta_i^\vee]$ and $B^\vee(\overline{\mathbb{Q}})[\varphi^\vee]$ are isomorphic to $\boldsymbol{\mu}_\ell$ as Galois modules for $\mathrm{Gal}_{\mathbb{Q}}$, we obtain isomorphisms from $H^1(\mathbb{Q}, E_i'(\overline{\mathbb{Q}})[\eta_i^\vee])$ and $H^1(\mathbb{Q}, B^\vee(\overline{\mathbb{Q}})[\varphi^\vee])$ to $H^1(\mathbb{Q}, \boldsymbol{\mu}_\ell)$. Composing with $\delta_{\mathbb{Q}}$ we get natural injective group homomorphisms

$$\operatorname{coker} \eta_{i,\mathbb{Q}}^\vee \hookrightarrow \mathbb{Q}^* / \mathbb{Q}^{*\ell}, \ \operatorname{coker} \varphi_{\mathbb{Q}}^\vee \hookrightarrow \mathbb{Q}^* / \mathbb{Q}^{*\ell}.$$

Even though these injective group homomorphisms are not uniquely determined, the images of these embeddings are independent of all choices made. We get the following commutative diagram.

$$\begin{array}{ccc} \operatorname{coker} \eta_{1,\mathbb{Q}}^\vee \times \operatorname{coker} \eta_{2,\mathbb{Q}}^\vee & \hookrightarrow & \mathbb{Q}^* / \mathbb{Q}^{*\ell} \times \mathbb{Q}^* / \mathbb{Q}^{*\ell} \\ \downarrow & & \downarrow \\ \operatorname{coker} \varphi_{\mathbb{Q}}^\vee & \hookrightarrow & \mathbb{Q}^* / \mathbb{Q}^{*\ell} \end{array} \tag{3.1}$$

In this diagram the natural surjection $\operatorname{coker}\eta_{1,\mathbb{Q}}^\vee \times \operatorname{coker}\eta_{2,\mathbb{Q}}^\vee \twoheadrightarrow \operatorname{coker}\varphi_{\mathbb{Q}}^\vee$ becomes $(x,y) \mapsto x^m/y$ as a map from $\mathbb{Q}^*/\mathbb{Q}^{*\ell} \times \mathbb{Q}^*/\mathbb{Q}^{*\ell}$ to $\mathbb{Q}^*/\mathbb{Q}^{*\ell}$, for a suitable $m \in \{1,\dots,\ell-1\}$. The image of $\operatorname{coker}\eta_{1,\mathbb{Q}}^\vee \times \operatorname{coker}\eta_{2,\mathbb{Q}}^\vee$ in the lower right group $\mathbb{Q}^*/\mathbb{Q}^{*\ell}$ is independent of m and n, and for determining the image we can simply set $m = 1$. The next proposition explains how to calculate the images of $\operatorname{coker}\eta_{i,\mathbb{Q}}^\vee$ in $\mathbb{Q}^*/\mathbb{Q}^{*\ell}$, i.e. how to calculate the upper horizontal map. Combining afterwards with $(x,y) \mapsto x/y$ gives $\operatorname{coker}\varphi_{\mathbb{Q}}^\vee$ as a subset of $\mathbb{Q}^*/\mathbb{Q}^{*\ell}$.

Proposition 3.2.1. *Let E and E' be elliptic curves over a number field K and $\eta : E \to E'$ an isogeny of prime degree ℓ. Assume that η has a K-kernel, i.e. $E(\overline{K})[\eta] = E(K)[\eta]$, and let $P \in E(K)$ be a generator of the kernel. Let $f_P \in K(E)$ be a K-rational function on E such that $\operatorname{div}(f_P) = \ell(P) - \ell(\mathcal{O})$. Then the following holds.*

(i) There exists a unique constant $c = c(f_P) \in K^*/K^{*\ell}$ such that

$$\operatorname{coker}\eta_K^\vee \to K^*/K^{*\ell}$$

$$[Q] \mapsto c \cdot f_P(Q) \bmod K^{*\ell}, \text{ for } Q \in E(K) \text{ with } Q \neq \mathcal{O}, P,$$

is a well-defined and injective group homomorphism.

(ii) The image of the map $c \cdot f_P$ is independent of the choice of the point P and function f_P and agrees with the image of the natural injection $\operatorname{coker}\eta_K^\vee \hookrightarrow K^*/K^{*\ell}$ described above.

(iii) The image of the map $c \cdot f_P$ lies in the finite set

$$K(S,\ell) := \{x \in K^*/K^{*\ell} \mid v_{\mathfrak{p}}(x) \equiv 0 \bmod \ell,\ \forall \mathfrak{p} \notin S\},$$

where S is the set of all primes $\mathfrak{p} \subset \mathcal{O}_K$, such that $\mathfrak{p}$ divides the degree of η or $\mathfrak{p}$ is a prime of bad reduction of E.

Proof. This is Exercise 10.1 in [Sil86]. □

Remark 3.2.2. By the Riemann-Roch Theorem, the vector space of functions $f_P \in K(E)$ with $\operatorname{div}(f_P) = \ell(P) - \ell(\mathcal{O})$ is 1-dimensional, hence such a function always exists. Given such a f_P it is easy to determine $c \in K^*/K^{*\ell}$ and to find the value for the image of P in $K^*/K^{*\ell}$, by using the fact that the map $c \cdot f_P \bmod K^{*\ell}$ is a group homomorphism. This is done explicitly in Propositions 3.3.4 and 3.3.12 and Lemmas 3.4.1 and 3.4.8.

Now we consider the remaining case, i.e. determining $\operatorname{coker}\varphi_{\mathbb{Q}}$. There is no natural injection of $\operatorname{coker}\eta_{i,\mathbb{Q}}$ into $\mathbb{Q}^*/\mathbb{Q}^{*\ell}$ as before, since $E_i(\overline{\mathbb{Q}})[\eta_i]$ is not isomorphic to $\boldsymbol{\mu}_\ell$ as a Galois module for $\mathrm{Gal}_{\mathbb{Q}}$. But $E_i(\overline{\mathbb{Q}})[\eta_i]$ is isomorphic to $\boldsymbol{\mu}_\ell$ as a Galois module for Gal_L, for $L := \mathbb{Q}(\boldsymbol{\mu}_\ell)$. Further, the natural restriction map

$$H^1(\mathbb{Q}, E_i(\overline{\mathbb{Q}})[\eta_i]) \to H^1(L, E_i(\overline{\mathbb{Q}})[\eta_i])$$

is injective, as the kernel, which equals $H^1(\mathrm{Gal}(L/\mathbb{Q}), E_i(\overline{\mathbb{Q}})[\eta_i])$, is trivial, since $[L : \mathbb{Q}] = \ell - 1$ is coprime to $\#E_i(\overline{\mathbb{Q}})[\eta_i] = \ell$. Using the isomorphism δ_L, we get

natural injections $\operatorname{coker}\eta_{i,\mathbb{Q}} \hookrightarrow H^1(\mathbb{Q}, E_i(\overline{\mathbb{Q}})[\eta_i]) \hookrightarrow H^1(L, E_i(\overline{\mathbb{Q}})[\eta_i]) \cong L^*/L^{*\ell}$ and hence we obtain the following commutative diagram.

$$\begin{array}{ccc} \operatorname{coker}\varphi_{\mathbb{Q}} & \hookrightarrow & L^*/L^{*\ell} \\ \downarrow & & \downarrow \\ \operatorname{coker}\eta_{1,\mathbb{Q}} \times \operatorname{coker}\eta_{2,\mathbb{Q}} & \hookrightarrow & L^*/L^{*\ell} \times L^*/L^{*\ell} \\ \downarrow & & \downarrow \\ \operatorname{coker}\psi_{\mathbb{Q}} & \hookrightarrow & L^*/L^{*\ell} \end{array} \tag{3.2}$$

In this diagram, the natural surjection $\operatorname{coker}\eta_{1,\mathbb{Q}} \times \operatorname{coker}\eta_{2,\mathbb{Q}} \twoheadrightarrow \operatorname{coker}\psi_{\mathbb{Q}}$ is $(x, y) \mapsto x^m/y$ as a map from $L^*/L^{*\ell} \times L^*/L^{*\ell}$ to $L^*/L^{*\ell}$, for a suitable $m \in \{1, \ldots, \ell-1\}$. As before, all images are independent of m and n, and so we can simply set $m = 1$ in our computations. Hence $\operatorname{coker}\varphi_{\mathbb{Q}}$ is easy to determine provided we know the images of $\operatorname{coker}\eta_{i,\mathbb{Q}}$ in $L^*/L^{*\ell}$.

To obtain a map which computes the images of $\operatorname{coker}\eta_{i,\mathbb{Q}}$ in $L^*/L^{*\ell}$, we observe that the dual isogeny $\eta_i^\vee : E_i' \to E_i$ has a L-kernel. Hence by Proposition 3.2.1, we need a generator $\check{P} \in E_i'(L)$ of $E_i'[\eta_i^\vee]$ and a L-rational function $f_{\check{P}} \in L(E_i')$, such that $\operatorname{div}(f_{\check{P}}) = \ell(\check{P}) - \ell(\mathcal{O})$. Again, the image of $\operatorname{coker}\eta_{i,\mathbb{Q}}$ in $L^*/L^{*\ell}$ lies in the finite set

$$L(S, \ell) := \{x \in L^*/L^{*\ell} \mid v_{\mathfrak{p}}(x) \equiv 0 \bmod \ell,\ \forall \mathfrak{p} \notin S\},$$

where S is the set of all primes $\mathfrak{p} \subset \mathcal{O}_L$, such that $\mathfrak{p}$ divides the degree of η or $\mathfrak{p}$ is a prime of bad reduction of E_i/L.

3.3. $N = 5$ and $N = 7$ ($k = 5, 7$)

For a prime $\ell \neq 2$, Mazur's theorem [Maz77b] tells us that the rational ℓ-primary part $E(\mathbb{Q})[\ell^\infty]$ of an elliptic curve $E/\mathbb{Q}$ is either trivial, or cyclic of order ℓ, where the non-trivial case can only happen if $\ell = 3, 5$ or 7. Further, if $E/\mathbb{Q}$ has a $\mathbb{Q}$-rational 5-torsion point, then its torsion subgroup is cyclic of order 5 or 10, and if $E/\mathbb{Q}$ has a $\mathbb{Q}$-rational 7-torsion point, then its torsion subgroup is cyclic of order 7. We use these standard facts without explicitly referring to them.

3.3.1. $N = 5$

The elliptic curves E over a number field K with a K-rational 5-torsion point P are parametrised by the Weierstraß equation

$$E : Y^2 + (d+1)XY + dY = X^3 + dX^2,\ P = (0, 0),$$

for $d \in K$, with the discriminant

$$\Delta = -d^5(d^2 + 11d - 1)$$

being different from zero. For $K = \mathbb{Q}$, this is exactly the case when $d \neq 0$ holds. Using Vélu's algorithm [Vél71] one obtains that the curve E is isogenous to the elliptic curve

$$E' : Y^2 + (d+1)XY + dY = X^3 + dX^2 + (5d^3 - 10d^2 - 5d)X + (d^5 - 10d^4 - 5d^3 - 15d^2 - d),$$

$$\Delta' = -d(d^2 + 11d - 1)^5,$$

via the isogeny $\eta : E \to E'$ whose kernel is generated by P. Hence, the kernel of η equals the following cyclic group

$$\langle P \rangle = \{\mathcal{O},\ P = (0,0),\ 2P = (-d, d^2),\ 3P = (-d, 0),\ 4P = (0, -d)\}.$$

If we write $d = u/v$, with $u, v \in \mathbb{Z}$ coprime, then E is isomorphic to

$$E_{u,v} : Y^2 + (u+v)XY + uv^2Y = X^3 + uvX^2,\ P = (0,0),$$

$$\Delta_{u,v} = -(uv)^5(u^2 + 11uv - v^2),$$

and E' is isomorphic to

$$E'_{u,v} : Y^2 + (u+v)XY + uv^2Y =$$

$$X^3 + uvX^2 + (5u^3v - 10u^2v^2 - 5uv^3)X + (u^5v - 10u^4v^2 - 5u^3v^3 - 15u^2v^4 - uv^5),$$

$$\Delta'_{u,v} = -uv(u^2 + 11uv - v^2)^5,$$

$$c'_{4,u,v} = u^4 - 228u^3v + 494u^2v^2 + 228uv^3 + v^4,$$

where $c'_{4,u,v}$ is the usual coefficients of a short Weierstraß equation of $E'_{u,v}$ as given for example in [Sil86, III.1].

To determine the local quotient, our approach is to use Theorem 3.1.2. For this, the reduction type of E at each prime p and the value of $|\eta'(0)|_p$ are necessary.

Lemma 3.3.1. *Let E be an elliptic curve as above parametrised by $d = u/v \in \mathbb{Q} \setminus \{0\}$, with $u, v \in \mathbb{Z}$ coprime, and let p be a prime number.*

(i) If $p|uv$ then E has split multiplicative reduction at p with $\ker \eta_p \not\subseteq E_0(\mathbb{Q}_p)$.

(ii) If $p|u^2 + 11uv - v^2$ then $\ker \eta_p \subseteq E_0(\mathbb{Q}_p)$. Further, E has split multiplicative reduction at p if and only if $p \equiv 1 \bmod 5$, additive reduction if and only if $p = 5$, and otherwise non-split multiplicative reduction with $p \equiv -1 \bmod 5$.

(iii) a) $v_5(u^2 + 11uv - v^2) \in \{0, 2, 3\}$,

b) $v_5(u^2 + 11uv - v^2) = 0 \ \Leftrightarrow\ u \not\equiv 2v \bmod 5$,

c) $v_5(u^2 + 11uv - v^2) = 3 \ \Leftrightarrow\ u \equiv 7v \bmod 25$,

d) $u \equiv 2v \bmod 5 \ \Rightarrow 5^4 \mid c'_{4,u,v}$

Proof. Most of part (i) and (ii) follow from Lemma 1.4 and the comment there-

after of [Fis00]. We give a more detailed proof. Consider the reduction-mod-p map $E(\mathbb{Q}_p) \to \tilde{\mathcal{E}}(\mathbb{F}_p)$ and the point $P = (0,0)$, which generates $\ker \eta_p$. If $p|uv$ then $\tilde{\mathcal{E}} : \overline{Y}^2 + \alpha\overline{XY} = \overline{X}^3$, for a non-zero $\alpha \in \mathbb{Z}/p\mathbb{Z}$. In particular, $\overline{P}$ is a node of $\tilde{\mathcal{E}}$ and the tangent cone is generated by $\overline{X} = -\alpha\overline{Y}$ and by $\overline{Y} = 0$. Thus the reduction type is split multiplicative and $P \notin E_0(\mathbb{Q}_p)$, which proves (i).

If $p|u^2 + 11uv - v^2$ then $\overline{P}$ is non-singular, hence $\ker \eta_p \subseteq E_0(\mathbb{Q}_p)$. Also $\overline{P}$ is non-trivial, therefore it has order 5. Since the order of $\overline{P}$ divides $\#\tilde{\mathcal{E}}_0(\mathbb{F}_p)$, which equals $p-1$ if the reduction is split multiplicative, $p+1$ if the reduction is non-split multiplicative, and p if the reduction is additive, we get (ii).

Part (iii) is an easy calculation. Any pair of integers u and v making the expression $u^2 + 11uv - v^2$ divisible by 5^4 are not coprime, as in this case both u and v are divisible by 5. □

Proposition 3.3.2. *Let $\eta : E \to E'$ be the isogeny described above, for the parameter $d = u/v \in \mathbb{Q} \setminus \{0\}$, with $u, v \in \mathbb{Z}$ coprime. Then*

$$|\eta'(0)|_p = \begin{cases} 1/5, & p = 5 \text{ and } u \equiv 7v \bmod 25 \\ 1, & \text{otherwise.} \end{cases}$$

Proof. If $p \neq 5$ or if p is a place of good or multiplicative reduction, then $|\eta'(0)|_p = 1$, by Theorem 2.3.7. If $p = 5$ is additive, then it follows from Lemma 3.3.1 and Exercise 7.1 of [Sil86], that the Weierstraß equation for $E_{u,v}$ is always minimal, and the one for $E'_{u,v}$ is not minimal if and only if $u \equiv 7v \bmod 25$. In this case, $v_5(\Delta'_{u,v}) = 15$ and $c'_{4,u,v}$ is divisible at least by 5^4. Hence, the change of variables $X \mapsto X/5^2$ and $Y \mapsto Y/5^3$ makes the Weierstraß equation for $E'_{u,v}$ minimal. We claim that $\eta(Z) = Z + ...$ as a power series in Z in a neighbourhood of $\mathcal{O}$, assuming that the equation for $E'_{u,v}$ is minimal. As $|\eta'(0)|_p$ equals the p-adic valuation of the leading coefficient of such a power series representation of η, we deduce that $\eta'(0) = 1$, and therefore $|\eta'(0)|_p = 1$. If the equation for $E'_{u,v}$ is not minimal, we have to replace Z by $5Z$, which gives $\eta(Z) = 5Z + \ldots$. It follows that $\eta'(0) = 5$ and $|\eta'(0)|_5 = 1/5$.

It remains to prove the claim. Set $\eta(X,Y) =: (\tilde{X}(X,Y), \tilde{Y}(X,Y))$. Then, by [Vél71], we have $-\tilde{X}(X,Y)/\tilde{Y}(X,Y) = p(X)/q(X,Y)$, where

$$p(X) := X(d+X)\left[d^4 + (3d^3+d^4)X + (3d^2+3d^3)X^2 + (d+3d^2-d^3)X^3 + 2dX^4 + X^5\right],$$

$$\begin{aligned} q(X,Y) := {} & d^6 + (5d^5+2d^6)X + (10d^4+8d^5+d^6)X^2 + (10d^3+13d^4+4d^5)X^3 \\ & + (5d^2+10d^3+4d^4)X^4 + (d+3d^2+d^3-d^4)X^5 \\ & + Y\left[2d^5 + (7d^4+d^5)X + (9d^3+3d^4)X^2 + (5d^2+3d^3+d^4)X^3 + (d-d^2-d^3)X^4 - 3dX^5 - X^6\right]. \end{aligned}$$

For $Z := -X/Y$, we have $X(Z) = Z^{-2} + \ldots$ and $Y(Z) = -Z^{-3} + \ldots$ as Laurent series for X and Y, see [Sil86, IV.1]. Therefore, $\eta(Z) = \frac{Z^{-14}+\ldots}{Z^{-15}+\ldots} = Z + \ldots$. □

The local quotient is completely determined by the above lemma and proposition together with Lemma 3.1.1 and Theorem 3.1.2.

Theorem 3.3.3. *Assume Setting 2.4.12 with $N = 5$. Let E_i be given by $d_i = u_i/v_i$, for $d_i \in \mathbb{Q} \setminus \{0\}$, with $u_i, v_i \in \mathbb{Z}$ coprime. If $p \in M_{\mathbb{Q}}$ is a place, then*

$$\frac{\#\operatorname{coker}\varphi_p}{\#\ker\varphi_p} = \begin{cases} 1/5, & p = \infty \\ 1/5, & p \mid u_1v_1u_2v_2 \\ 5, & p \mid \gcd(u_1^2 + 11u_1v_1 - v_1^2, u_2^2 + 11u_2v_2 - v_2^2),\ p \equiv 1(5) \\ 5, & u_1 \equiv 7v_1 \bmod 25, u_2 \equiv 7v_2 \bmod 25,\ p = 5 \\ 1, & \textit{otherwise}. \end{cases}$$

Next comes the global quotient. It is possible to use Proposition 3.2.1 to calculate $\operatorname{coker}\eta_{i,\mathbb{Q}}^{\vee}$ in $\mathbb{Q}^*/\mathbb{Q}^{*5}$, as η_i has a $\mathbb{Q}$-kernel with generating point $P_i = (0,0)$. By Mazur's theorem, $\operatorname{coker}\eta_{i,\mathbb{Q},\mathrm{tors}}^{\vee}$ is generated by P_i, independent of the structure of $E_i(\mathbb{Q})_{\mathrm{tors}}$.

Proposition 3.3.4. *For $P = (0,0)$ set*

$$f_P := -X^2 + XY + Y \in K(E).$$

The image of the natural embedding $\operatorname{coker}\eta_{\mathbb{Q}}^{\vee} \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*5}$ equals the image of

$$f_P(X,Y) \bmod \mathbb{Q}^{*5}, \textit{ for } Q = (X,Y) \neq \mathcal{O}, P.$$

By linearity $f_P(P) = d^4$, and $f_P(\operatorname{coker}\eta_{\mathbb{Q},\mathrm{tors}}^{\vee}) = \langle d \rangle$ in $\mathbb{Q}^*/\mathbb{Q}^{*5}$.

Proof. For functions $X, Y, X + Y + d \in K(E)$, one easily sees that $\operatorname{div}(X) = (P) + (4P) - 2(\mathcal{O})$, $\operatorname{div}(Y) = 2(P) + (3P) - 3(\mathcal{O})$, and $\operatorname{div}(X + Y + d) = 2(3P) + (4P) - 3(\mathcal{O})$. Multiplying $(XY^2)/(X + Y + d)$ with $(-Y - dX)/(-Y - dX)$ yields $-X^2 + XY + Y$ in $K(E)$, and thus $\operatorname{div}(f_P) = 5(P) - 5(\mathcal{O})$. By Proposition 3.2.1 we obtain that $c \cdot f_P$ is the function we are looking for. Since $(f_P(2P))^2 = f_P(4P)$, we deduce $c = 1$ and that $f_P(P) \equiv f_P(2P)^3 \equiv d^4 \bmod \mathbb{Q}^{*5}$. □

Corollary 3.3.5. *With notation as above, $E'(\mathbb{Q})[5] \cong \mathbb{Z}/5\mathbb{Z} \Leftrightarrow d \in \mathbb{Q}^{*5}$.*

Proof. We have that $E'(\mathbb{Q})[5]$ is non-trivial if and only if $\operatorname{coker}\eta_{\mathbb{Q}}^{\vee}$ is trivial on the torsion part, i.e., the injective map $\eta_{\mathbb{Q},\mathrm{tors}}^{\vee} : E'(\mathbb{Q})_{\mathrm{tors}} \to E(\mathbb{Q})_{\mathrm{tors}}$ is an isomorphism. The cokernel of $\eta_{\mathbb{Q},\mathrm{tors}}^{\vee}$ is generated by d in $\mathbb{Q}^*/\mathbb{Q}^{*5}$. Hence $E'(\mathbb{Q})[5]$ is non-trivial if and only if d is trivial in $\mathbb{Q}^*/\mathbb{Q}^{*5}$. □

Now we calculate $\operatorname{coker}\eta_{\mathbb{Q}}$ in L^*/L^{*5}, for $L := \mathbb{Q}(\xi)$, with $\xi \in \boldsymbol{\mu}_5$ a primitive fifth root of unity. Fix a generator $\check{P}$ of $E'(\overline{\mathbb{Q}})[\eta^{\vee}]$. Since $\check{P} \in E'(L)$, we have that $E'(L)[\eta^{\vee}] \cong \mathbb{Z}/5\mathbb{Z}$ and hence $(E', \check{P})$ is isomorphic over L to a pair $(E_{\tilde{d}}, (0,0))$, where $E_{\tilde{d}}$ denotes the elliptic curve over L with a L-rational 5-torsion point $(0,0)$ with respect to the parameter $\tilde{d} \in L$. Such a L-isomorphism $\epsilon : (E', \check{P}) \tilde{\to} (E_{\tilde{d}}, (0,0))$

is given by four values $r, s, t \in L$ and $w \in L^*$ and has the form $X = w^2X' + r$ and $Y = w^3Y' + w^2sX' + t$ [Sil86, III.1]. Having such an isomorphism ϵ and the formula of f_P from Proposition 3.3.4, we can determine $f_{\check{P}}$, since

$$f_{\check{P}}(X, Y) \equiv \epsilon^* f_P(X', Y') \bmod L^{*5}.$$

To obtain ϵ we use [Sil86, III Table 1.2]. As a_6 of the Weierstraß equation of $E_{\tilde{d}}$ vanishes, we get $(r, t) = \check{P}$. The kernel polynomial of the dual isogeny $\eta^\vee : E' \to E$ is

$$X^2 + (d^2 + d + 1)X + \frac{1}{5}(d^4 - 3d^3 - 26d^2 + 8d + 1);$$

thus, for $\vartheta := \xi + \xi^{-1} = (\sqrt{5} - 1)/2$, we may choose

$$r = \frac{1}{5}[(-\vartheta - 3)d^2 + (-11\vartheta - 8)d + (\vartheta - 2)] \in \mathbb{Q}(\vartheta) = \mathbb{Q}(\sqrt{5}),$$

$$t = \frac{1}{5}[(\xi^2 + 2\xi + 2)d^3 + (\xi^3 + 10\xi^2 + 23\xi + 11)d^2$$
$$+(11\xi^3 - 12\xi^2 + 9\xi + 2)d + (-\xi^3 + \xi^2 - \xi + 1)] \in L.$$

Since a_4 of $E_{\tilde{d}}$ also vanishes we deduce

$$s = \frac{1}{5}[(-4\xi^3 - 3\xi^2 - 7\xi - 6)d + (3\xi^3 - 4\xi^2 - \xi - 3)],$$

and since $a_3 = a_2$ we deduce

$$w = \frac{1}{5}[(-\xi^3 - 7\xi^2 - 8\xi - 4)d + (7\xi^3 - \xi^2 + 6\xi + 3)].$$

Also one can use the conditions on the a_i to calculate $\tilde{d} = \frac{(5\vartheta-3)d+1}{d-(5\vartheta-3)}$. All in all we have described an algorithm to compute $f_{\check{P}}$. If one multiplies the obtained result by w^5 to get rid of denominators one obtains

$$f_{\check{P}}(X, Y) = \frac{1}{25}[(3 + 6\xi - \xi^2 + 7\xi^3) + (80 + 235\xi - 60\xi^2 + 245\xi^3)d$$
$$+(220 + 465\xi + 185\xi^2 + 205\xi^3)d^2 + (15 + 55\xi - 55\xi^2 + 160\xi^3)d^3$$
$$+(140 + 280\xi + 245\xi^2 + 35\xi^3)d^4 + (-4 - 8\xi - 7\xi^2 - \xi^3)d^5]$$
$$+[(-1 + \xi - \xi^2) + (3 + 9\xi + 2\xi^2 + 2\xi^3)d + (2 + 6\xi + 8\xi^2 - 3\xi^3)d^2$$
$$+(-1 - \xi + \xi^3)d^3]X + [(-\xi + \xi^2 - 2\xi^3) + (2 + 3\xi + 2\xi^2 + \xi^3)d]X^2$$
$$+[(-3 - 2\xi^2 - 2\xi^3) + (-1 - 3\xi^2 - 3\xi^3)d + (-1 + 2\xi^2 + 2\xi^3)d^2]Y + XY \in L(E').$$

Now we express the torsion quotient in terms of the pair (d_1, d_2).

Proposition 3.3.6. *Assume Setting 2.4.12 with $N = 5$. Let E_i be given by $d_i \in \mathbb{Q} \setminus \{0\}$. Then the following holds.*

$$\frac{\#A(\mathbb{Q})_{\text{tors}}\,\#A^\vee(\mathbb{Q})_{\text{tors}}}{\#B(\mathbb{Q})_{\text{tors}}\,\#B^\vee(\mathbb{Q})_{\text{tors}}} = \begin{cases} 1 \text{ or } 5, & d_1, d_2 \in \mathbb{Q}^{*5} \\ 5^2, & d_i \in \mathbb{Q}^{*5}, d_j \notin \mathbb{Q}^{*5}, i \neq j \\ 5^2, & \langle 1\rangle \neq \langle d_1\rangle = \langle d_2\rangle \neq \langle 1\rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*5} \\ 5^3, & \langle 1\rangle \neq \langle d_1\rangle \neq \langle d_2\rangle \neq \langle 1\rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*5}. \end{cases}$$

To be more precise, in case both $d_i \in \mathbb{Q}^{*5}$, set $d_i =: \delta_i^5$, for $\delta_i \in \mathbb{Q}^*$, and define $\zeta_1 := -\xi^4(\xi + 1)$, $\zeta_2 := -\xi(\xi+1)$, $\zeta_3 := -\xi^3(\xi+1)$ and $\zeta_4 := -(\xi+1)$, where $\xi \in \boldsymbol{\mu}_5$ is a primitive fifth root of unity. Then the torsion quotient equals 1 if and only if

$$\left\langle \prod_{j=1}^{4} (\delta_1 + \zeta_j)^j (\delta_1 - 1/\zeta_j)^j \right\rangle = \left\langle \prod_{j=1}^{4} (\delta_2 + \zeta_j)^j (\delta_2 - 1/\zeta_j)^j \right\rangle \text{ in } L^*/L^{*5}.$$

Proof. The torsion quotient equals $5 \cdot \#\operatorname{coker} \varphi^\vee_{\mathbb{Q},\text{tors}} / \#\operatorname{coker} \varphi_{\mathbb{Q},\text{tors}}$. We have seen above that $E'(\mathbb{Q})[5] \cong \mathbb{Z}/5\mathbb{Z}$ if and only if $d \in \mathbb{Q}^{*5}$. Hence, $\operatorname{coker} \eta_{i,\mathbb{Q},\text{tors}}$ is trivial in case $d_i \notin \mathbb{Q}^{*5}$, otherwise it is 1-dimensional. Consider Diagrams (3.1) and (3.2). Looking at the kernel of $(x, y) \mapsto x/y$ gives that $\operatorname{coker} \varphi_{\mathbb{Q},\text{tors}}$ might have five elements in case $d_1,\ d_2 \in \mathbb{Q}^{*5}$, and is trivial otherwise. Since $\operatorname{coker} \eta^\vee_{i,\mathbb{Q},\text{tors}}$ is generated by $d_i \mod \mathbb{Q}^{*5}$, and the map onto $\operatorname{coker} \varphi^\vee_{\mathbb{Q},\text{tors}}$ is given by $(x, y) \mapsto x/y$, we get

$$\#\operatorname{coker} \varphi^\vee_{\mathbb{Q},\text{tors}} = \begin{cases} 1, & d_1, d_2 \in \mathbb{Q}^{*5} \\ 5, & d_i \in \mathbb{Q}^{*5}, d_j \notin \mathbb{Q}^{*5}, i \neq j \\ 5, & \langle 1\rangle \neq \langle d_1\rangle = \langle d_2\rangle \neq \langle 1\rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*5} \\ 5^2, & \langle 1\rangle \neq \langle d_1\rangle \neq \langle d_2\rangle \neq \langle 1\rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*5}, \end{cases}$$

which finishes the first part. For the second part, note that if $d_i = \delta_i^5$, then $E'(\mathbb{Q})[5]$ is generated by the point $P_i' = (x_i', y_i')$, where

$$x_i' = \delta_i + 2\delta_i^2 + 3\delta_i^2 + 5\delta_i^4 + 2\delta_i^5 + 2\delta_i^6 - \delta_i^7 + \delta_i^8,$$

$$y_i' = \delta_i^2 + 3\delta_i^3 + 5\delta_i^4 + 11\delta_i^5 + 13\delta_i^6 + 10\delta_i^7 + \delta_i^8 - \delta_i^{10} + \delta_i^{11} + \delta_i^{12}.$$

The image of $\langle P_i' \rangle$ under f_T in L^*/L^{*5}, i.e. the image of $\operatorname{coker} \eta_{i,\mathbb{Q},\text{tors}}$ in L^*/L^{*5}, is $\left\langle \prod_{j=1}^4 (\delta_i + \zeta_j)^j (\delta_i - 1/\zeta_j)^j \right\rangle$, which completes the second part. □

Finally, we give two unconditional examples of an abelian surface $B/\mathbb{Q}$ of rank 0, respectively of rank 1, such that $\#Ш(B/\mathbb{Q}) = 5$.

Example 3.3.7. If $d_1 = u_1/v_1 = 1/11$, $d_2 = u_2/v_2 = 2/9$, then $\#Ш(B/\mathbb{Q}) = 5$.

Proof. We start with the local quotient. There are three different primes dividing $u_1v_1u_2v_2 = 2 \cdot 3^2 \cdot 11$. We also have the contribution of the prime at infinity,

and no contribution from any other prime, as $u_i \not\equiv 7 \cdot v_i \bmod 25$ for both i, and $\gcd(u_1^2 + 11u_1v_1 - v_1^2, u_2^2 + 11u_2v_2 - v_2^2) = 1$. Hence the local quotient equals $1/5^4$. Both elliptic curves E_i have analytic rank equal to 0, hence we know that $Ш(A/\mathbb{Q})$ and $Ш(B/\mathbb{Q})$ are finite and that the global quotient equals the torsion quotient. Thus the global quotient equals 5^3. We conclude that $\#Ш(B/\mathbb{Q}) = 5 \cdot \#Ш(A/\mathbb{Q})$.

It remains to show that both $Ш(E_i/\mathbb{Q})$ are trivial. The predicted size by the Birch and Swinnerton-Dyer formula is 1. Both E_i are non-CM curves of conductor at most 1000, hence we can apply [Ste09, Theorem 3.31 and Theorem 4.4]. This implies that $\#Ш(E_i/\mathbb{Q})[p^\infty] = 1$, for all primes $p \neq 5$, as the primes occurring as the degrees of cyclic isogenies or dividing any Tamagawa number are only 2 and 5. From [Fis00, Theorem 1 or Table 3 in the Appendix] it follows that $\mathrm{Sel}^{\eta_i}(E_i/\mathbb{Q}) = 0$ and $\mathrm{Sel}^{\eta_i^\vee}(E_i'/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$, for both i. As $\operatorname{coker} \eta_{i,\mathbb{Q}} = 0$ and $\operatorname{coker} \eta_{i,\mathbb{Q}}^\vee \cong \mathbb{Z}/5\mathbb{Z}$, we get $Ш(E_i/\mathbb{Q})[\eta_i] = Ш(E_i'/\mathbb{Q})[\eta_i^\vee] = 0$ and $Ш(E_i/\mathbb{Q})[5] = 0$. Hence $Ш(E_i/\mathbb{Q}) = 0$. □

Example 3.3.8. If $d_1 = u_1/v_1 = 1/10$, $d_2 = u_2/v_2 = 3/1$, then $\#Ш(B/\mathbb{Q}) = 5$.

Proof. We have $u_1v_1u_2v_2 = 2 \cdot 3 \cdot 5$, $u_i \not\equiv 7 \cdot v_i \bmod 25$, for both i, and $\gcd(u_1^2 + 11u_1v_1 - v_1^2, u_2^2 + 11u_2v_2 - v_2^2) = 1$. Hence the local quotient equals $1/5^4$. The elliptic curve E_1 is of analytic rank 0 and E_2 of analytic rank 1. A generator of the free part of $E_2(\mathbb{Q})$ is the point $(-6, 12)$. We start determining $\operatorname{coker} \eta_{i,\mathbb{Q}}^\vee$ as a subset of $\mathbb{Q}^*/\mathbb{Q}^{*5}$. For the first curve this equals just the torsion part of the cokernel, hence $\operatorname{coker} \eta_{1,\mathbb{Q}}^\vee$ is generated by $\{2 \cdot 5\}$. The second cokernel is generated by the image of the torsion point, which is 3, and by the image of $(-6, 12)$ under $f = -X^2 + XY + Y$, which is $-3 \cdot 2^5 \equiv 3 \bmod \mathbb{Q}^{*5}$. Therefore $\operatorname{coker} \eta_{2,\mathbb{Q}}^\vee$ is generated only by $\{3\}$ and hence $\operatorname{coker} \varphi_{\mathbb{Q}}^\vee$ has dimension equal to 2. Since neither d_i are fifth powers, we get that the dimension of $\operatorname{coker} \eta_{1,\mathbb{Q}}$ equals 0 and the dimension of $\operatorname{coker} \eta_{2,\mathbb{Q}}$ equals 0 or 1, thus the dimension of $\operatorname{coker} \varphi_{\mathbb{Q}}$ equals 0. We conclude that the global quotient equals 5^3, which gives $\#Ш(B/\mathbb{Q}) = 5 \cdot \#Ш(A/\mathbb{Q})$. Now one can use a similar strategy as in the previous example to show that $Ш(A/\mathbb{Q})$ is trivial. □

3.3.2. $N = 7$

The situation for $N = 7$ is very similar to the case $N = 5$, so we mostly just state the results. The elliptic curves E with a rational 7-torsion point P are parametrised by the Weierstraß equation

$$E : Y^2 + (1 + d - d^2)XY + (d^2 - d^3)Y = X^3 + (d^2 - d^3)X^2,\ P = (0, 0),$$

$$\Delta = -d^7(1 - d)^7(d^3 - 8d^2 + 5d + 1).$$

Thus for $K = \mathbb{Q}$ we have $d \neq 0, 1$. The isogenous curve is

$$E' : Y^2 + (1 + d - d^2)XY + (d^2 - d^3)Y =$$

$$X^3 + (d^2 - d^3)X^2 + (5d - 35d^2 + 70d^3 - 70d^4 + 35d^5 - 5d^7)X$$

$$+(d - 19d^2 + 94d^3 - 258d^4 + 393d^5 - 343d^6 + 202d^7 - 107d^8 + 46d^9 - 8d^{10} - d^{11}),$$
$$\Delta' = -d(1-d)(d^3 - 8d^2 + 5d + 1)^7,$$

and the points in the kernel of $\eta : E \to E'$ are

$$\langle P \rangle = \{\mathcal{O},\ P = (0,0),\ 2P = (d^3 - d^2, d^5 - 2d^4 + d^3),\ 3P = (d^2 - d, d^3 - 2d^2 + d),$$
$$4P = (d^2 - d, d^4 - 2d^3 + d^2),\ 5P = (d^3 - d^2, 0),\ 6P = (0, d^3 - d^2)\}.$$

If we write $d = u/v$, with $u, v \in \mathbb{Z}$ coprime, we get

$$E_{u,v} : Y^2 + ((v-u)(v+u) + uv)XY + (v-u)u^2v^3Y = X^3 + (v-u)u^2vX^2,\ P = (0,0),$$
$$\Delta_{u,v} = -(uv)^7(v-u)^7(u^3 - 8u^2v + 5uv^2 + v^3),$$
$$E'_{u,v} : Y^2 + ((v-u)(v+u) + uv)XY + (v-u)u^2v^3Y =$$
$$X^3 + (v-u)u^2vX^2 + (-5u^7v + 35u^5v^3 - 70u^4v^4 + 70u^3v^5 - 35u^2v^6 + 5uv^7)X$$
$$-u^{11}v - 8u^{10}v^2 + 46u^9v^3 - 107u^8v^4 + 202u^7v^5 - 343u^6v^6$$
$$+393u^5v^7 - 258u^4v^8 + 94u^3v^9 - 19u^2v^{10} + uv^{11},$$
$$\Delta'_{u,v} = -uv(v-u)(u^3 - 8u^2v + 5uv^2 + v^3)^7.$$
$$c'_{4,u,v} = u^8 + 228u^7v + 42u^6v^2 - 1736u^5v^3 + 3395u^4v^4$$
$$-3360u^3v^5 + 1666u^2v^6 - 236uv^7 + v^8.$$

As before, to determine the local quotient we have to know the reduction type of E at p and the value $|\eta'(0)|_p$.

Lemma 3.3.9. *Let E be an elliptic curve as above parametrised by $d = u/v \in \mathbb{Q} \setminus \{0,1\}$, with $u, v \in \mathbb{Z}$ coprime, and let p be a prime number.*

(i) If $p | uv(v-u)$ then E has split multiplicative reduction at p with $\ker \eta_p \nsubseteq E_0(\mathbb{Q}_p)$.

(ii) If $p | u^3 - 8u^2v + 5uv^2 + v^3$ then $\ker \eta_p \subseteq E_0(\mathbb{Q}_p)$. Further, E has split multiplicative reduction at p if and only if $p \equiv 1 \bmod 7$, additive reduction if and only if $p = 7$, and otherwise non-split multiplicative reduction with $p \equiv -1 \bmod 7$.

(iii) a) $v_7(u^3 - 8u^2v + 5uv^2 + v^3) \in \{0, 2\}$,

b) $v_7(u^3 - 8u^2v + 5uv^2 + v^3) = 2 \Leftrightarrow u \equiv 5v \bmod 7$,

c) $u \equiv 5v \bmod 7 \Rightarrow 7^6 \mid c'_{4,u,v}$.

Proof. Analogous to the proof of Lemma 3.3.1. □

Proposition 3.3.10. *Let $\eta : E \to E'$ be the isogeny described above, for the parameter $d = u/v \in \mathbb{Q} \setminus \{0,1\}$, with $u, v \in \mathbb{Z}$ coprime. Then*

$$|\eta'(0)|_p = \begin{cases} 1/7, & p = 7 \text{ and } u \equiv 5v \bmod 7 \\ 1, & \text{otherwise.} \end{cases}$$

Proof. Analogous to the proof of Proposition 3.3.2. □

Hence, for the local quotient we have the following

Theorem 3.3.11. *Assume Setting 2.4.12 with $N = 7$. Let E_i be given by $d_i = u_i/v_i$, for $d_i \in \mathbb{Q} \setminus \{0,1\}$, with $u_i, v_i \in \mathbb{Z}$ coprime. If $p \in M_{\mathbb{Q}}$ is a place, then*

$$\frac{\#\operatorname{coker}\varphi_p}{\#\ker\varphi_p} = \begin{cases} 1/7, & p = \infty \\ 1/7, & p \mid u_1v_1u_2v_2(v_1-u_1)(v_2-u_2) \\ 7, & p \mid \gcd(u_1^3 - 8u_1^2v_1 + 5u_1v_1^2 + v_1^3, u_2^3 - 8u_2^2v_2 + 5u_2v_2^2 + v_2^3),\ p \equiv 1(7) \\ 7, & u_1 \equiv 5v_1 \bmod 7, u_2 \equiv 5v_2 \bmod 7,\ p = 7 \\ 1, & \textit{otherwise}. \end{cases}$$

Next comes the global quotient.

Proposition 3.3.12. *For $P = (0,0)$ set*

$$f_P := d^2X^2 + X^3 + dX^3 - d^2Y - XY - 2dXY - X^2Y \in K(E).$$

The image of the natural embedding $\operatorname{coker}\eta_{\mathbb{Q}}^{\vee} \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*7}$ equals the image of

$$f_P(X,Y) \bmod \mathbb{Q}^{*7}, \textit{ for } Q = (X,Y) \neq \mathcal{O}, P.$$

By linearity $f_P(P) = d^3(d-1)^6$, and $f_P(\operatorname{coker}\eta_{\mathbb{Q},\mathrm{tors}}^{\vee}) = \langle d(d-1)^2\rangle$ in $\mathbb{Q}^*/\mathbb{Q}^{*7}$.

Proof. We have that $\operatorname{div}(X) = (P) + (6P) - 2(\mathcal{O})$, $\operatorname{div}(Y) = 2(P) + (5P) - 3(\mathcal{O})$, $\operatorname{div}(Xd-1) - Y) = (P) + 2(3P) - 3(\mathcal{O})$, and $\operatorname{div}(X + Y - d^3 + d^2) = (3P) + (5P) + (6P) - 3(\mathcal{O})$, hence $\operatorname{div}(Y^2X^2(X(d-1)-Y)/(X+Y-d^3+d^2)^2) = 7(P) - 7(\mathcal{O})$. Multiplying with $(-Y-(1+d-d^2)X-(d^2-d^3))/(-Y-(1+d-d^2)X-(d^2-d^3))$ gives $d^2X^2 + X^3 + dX^3 - d^2Y - XY - 2dXY - X^2Y$. Proceed as in Proposition 3.3.4. □

Corollary 3.3.13. *With notation as above, $E'(\mathbb{Q})[7] = 0$.*

Proof. As in Corollary 3.3.5, $E'(\mathbb{Q})[7]$ is non-trivial if and only if $d(d-1)^2$ is trivial in $\mathbb{Q}^*/\mathbb{Q}^{*7}$, which is equivalent to d and $d-1$ being a seventh power, for $d \in \mathbb{Q} \setminus \{0,1\}$. But Fermat's Last Theorem for exponent 7 says that this never happens. □

Now set $L := \mathbb{Q}(\xi)$, for $\xi \in \boldsymbol{\mu}_7$ a primitive seventh root of unity. As in case $N = 5$, we want to compute a function $f_{\check{P}}$, which calculates the image of $\operatorname{coker}\eta_{\mathbb{Q}}$ in L^*/L^{*7}, and which depends on a point $\check{P} = (r,t) \in E'(\overline{\mathbb{Q}})[\eta^{\vee}]$. The coefficients r, t, s, w for the L-isomorphism $\epsilon : (E', \check{P}) \tilde{\to} (E_{\tilde{d}}, (0,0))$ can be computed in the same manner as before. The kernel polynomial of the dual isogeny $\eta^{\vee} : E' \to E$ is

$$\frac{1}{7}(d^{12} + 3d^{11} - 51d^{10} + 185d^9 - 767d^8 + 2097d^7 - 2835d^6$$

$$+1738d^5 - 295d^4 - 116d^3 + 55d^2 - 15d + 1)$$

$$+(d^8 - d^7 - 14d^6 + 32d^5 - 29d^4 + 7d^3 + 11d^2 - 7d + 1)X$$
$$+(2d^4 - 5d^3 + 6d^2 - 3d + 2)X^2 + X^3,$$

hence for $\vartheta := \xi + \xi^{-1}$ we may choose

$$r = \frac{1}{7}[(3\vartheta^2 + 2\vartheta - 9)d^4 + (-25\vartheta^2 - 19\vartheta + 47)d^3$$
$$+(23\vartheta^2 + 34\vartheta - 41)d^2 + (-2\vartheta^2 - 13\vartheta + 6)d + (-\vartheta^2 - 3\vartheta - 4)] \in \mathbb{Q}(\vartheta),$$
$$t = \frac{1}{7}[(-3\xi^5 - 6\xi^4 - \xi^3 - \xi^2 - 5\xi - 5)d^6 + (28\xi^5 + 59\xi^4 + 7\xi^3 + 10\xi^2 + 45\xi + 33)d^5$$
$$+(-52\xi^5 - 119\xi^4 + 6\xi^3 - 16\xi^2 - 62\xi - 51)d^4 + (56\xi^5 + 54\xi^4 - 35\xi^3 - 37\xi^2 - 9\xi + 13)d^3$$
$$+(-13\xi^5 + 30\xi^4 + 54\xi^3 + 75\xi^2 + 60\xi + 32)d^2 + (-10\xi^5 - 16\xi^4 - 22\xi^3 - 25\xi^2 - 22\xi - 17)d$$
$$+(-\xi^5 - 3\xi^4 - 5\xi^3 - 6\xi^2 - 5\xi - 1)] \in L.$$

Using the conditions on the a_i gives

$$s = \frac{1}{7}[(3\xi^5 + 6\xi^4 - 5\xi^3 - 2\xi^2 + \xi + 4)d^2 + (-16\xi^5 - 11\xi^4 - 6\xi^3 - \xi^2 - 17\xi - 12)d$$
$$+(5\xi^5 + 3\xi^4 + 8\xi^3 + 6\xi^2 + 11\xi + 2)],$$
$$w = \frac{1}{7}[(-3\xi^5 - 6\xi^4 - \xi^3 - \xi^2 - 5\xi - 5)d^6 + (28\xi^5 + 59\xi^4 + 7\xi^3 + 10\xi^2 + 45\xi + 33)d^5$$
$$+(-52\xi^5 - 119\xi^4 + 6\xi^3 - 16\xi^2 - 62\xi - 51)d^4 + (56\xi^5 + 54\xi^4 - 35\xi^3 - 37\xi^2 - 9\xi + 13)d^3$$
$$+(-13\xi^5 + 30\xi^4 + 54\xi^3 + 75\xi^2 + 60\xi + 32)d^2 + (-10\xi^5 - 16\xi^4 - 22\xi^3 - 25\xi^2 - 22\xi - 17)d$$
$$+(-\xi^5 - 3\xi^4 - 5\xi^3 - 6\xi^2 - 5\xi - 1)],$$
$$\tilde{d} = \frac{(\vartheta^2 + 3\vartheta + 2)d - (\vartheta^2 + 3\vartheta + 1)}{d - (\vartheta^2 + 3\vartheta + 2)}.$$

Now putting everything together gives

$$f_{\check{p}} \equiv w^7 \cdot f_P((X - r)/w^2, (Y - t - s(X - r))/w^3)$$
$$= w^3\tilde{d}^2(X - r)^2 + w(X - r)^3 + w\tilde{d}(X - r)^3 - w^4\tilde{d}^2(Y - t - s(X - r))$$
$$-w^2(X - r)(Y - t - s(X - r)),$$

which yields a page long formula for $f_{\check{p}}$. For the torsion quotient we get the following

Proposition 3.3.14. *Assume Setting 2.4.12 with $N = 7$. Let E_i be given by $d_i \in \mathbb{Q} \setminus \{0, 1\}$. Then the following holds.*

$$\frac{\#A(\mathbb{Q})_{\text{tors}}\,\#A^\vee(\mathbb{Q})_{\text{tors}}}{\#B(\mathbb{Q})_{\text{tors}}\,\#B^\vee(\mathbb{Q})_{\text{tors}}} = \begin{cases} 7^2, & \langle d_1(d_1 - 1)^2\rangle = \langle d_2(d_2 - 1)^2\rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*7} \\ 7^3, & \text{otherwise.} \end{cases}$$

Proof. As $A(\mathbb{Q})[7^\infty] \cong (\mathbb{Z}/7\mathbb{Z})^2$ and $A'(\mathbb{Q})[7^\infty] = 0$, we have $B(\mathbb{Q})[7^\infty] \cong \mathbb{Z}/7\mathbb{Z}$, and hence $\#\operatorname{coker} \varphi_{\mathbb{Q},\mathrm{tors}} = 1$. We know that $\operatorname{coker} \eta^\vee_{i,\mathbb{Q},\mathrm{tors}}$ is generated by $d_i(d_i-1)^2$ in $\mathbb{Q}^*/\mathbb{Q}^{*7}$ and as the product of these two cokernels maps surjectively onto $\operatorname{coker} \varphi^\vee_{\mathbb{Q},\mathrm{tors}}$ via the map $(x,y) \mapsto x/y$, we conclude that

$$\#\operatorname{coker} \varphi^\vee_{\mathbb{Q},\mathrm{tors}} = \begin{cases} 7, & \langle d_1(d_1-1)^2\rangle = \langle d_2(d_2-1)^2\rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*7} \\ 7^2, & \text{otherwise,} \end{cases}$$

which completes the proof. □

We finish by giving an unconditional example of an abelian surface $B/\mathbb{Q}$ of rank equal to 0, such that $\#Ш(B/\mathbb{Q}) = 7$.

Example 3.3.15. If $d_1 = u_1/v_1 = 1/3$, $d_2 = u_2/v_2 = 1/4$, then $\#Ш(B/\mathbb{Q}) = 7$.

Proof. We have $u_1v_1u_2v_2(v_1-u_1)(v_2-u_2) = 2^3\cdot 3^2$, $u_1 \equiv 5\cdot v_1 \bmod 7$, $u_2 \not\equiv 5\cdot v_2 \bmod 7$, and $\gcd(u_1^3 - 8u_1^2v_1 + 5u_1v_1^2 + v_1^3, u_2^3 - 8u_2^2v_2 + 5u_2v_2^2 + v_2^3) = 1$. Hence the local quotient equals $1/7^3$. Both elliptic curves E_i have analytic rank equal to 0, hence we know that $Ш(A/\mathbb{Q})$ and $Ш(B/\mathbb{Q})$ are finite and that the global quotient equals the torsion quotient. For $a = 4$ we have that $d_1^a(d_1-1)^{2a} \equiv 2\cdot 3^2 \equiv d_2(d_2-1)^2 \bmod \mathbb{Q}^{*7}$, thus the global quotient equals 7^2. We conclude that $7\cdot \#Ш(A/\mathbb{Q}) = \#Ш(B/\mathbb{Q})$. As in the examples of $N = 5$, one can use [Ste09] and [Fis00] to show that $Ш(A/\mathbb{Q})$ is trivial. □

3.4. $N = 6$ and $N = 10$ ($k = 1, 2, 3, 6, 10$)

We start with the case $N = 6$ and present examples for $k = 1, 2, 3, 6$. Then we have a look at the case $N = 10$ to give an example for $k = 10$.

3.4.1. $N = 6$

The elliptic curves E over a number field K having a rational 6-torsion point P are parametrised by

$$E : Y^2 + (d+1)XY - d(d-1)Y = X^3 - d(d-1)X^2,\ P = (0,0),$$

$$\Delta = d^6(9d-1)(d-1)^3,$$

for $d \in K \setminus \{0, 1, 1/9\}$. If $d = u/v$, with $u, v \in \mathbb{Z}$ coprime, then E is isomorphic to

$$E_{u,v} : Y^2 + (u+v)XY - uv(u-v)Y = X^3 - u(u-v)X^2,\ P = (0,0),$$

$$\Delta_{u,v} = u^6v^2(9u-v)(u-v)^3.$$

Denote by $\eta : E \to E'$ the cyclic isogeny of degree 6, whose kernel is $\langle P\rangle$. Then

$$E' : Y^2 + (d+1)XY - d(d-1)Y = X^3 - d(d-1)X^2$$

$$-5(3d^3 - 4d^2 + d + 1)dX - (19d^5 - 33d^4 + 18d^3 - 22d^2 + 14d + 1)d.$$

The points of the kernel of η are

$$\{\mathcal{O},\ P = (0,0),\ 2P = (d(d-1), -d^2(d-1)),\ 3P = (-d, d^2),$$

$$4P = (d(d-1), 0),\ 5P = (0, d(d-1))\}.$$

Let $\check{P}$ denote a generator of the kernel of the dual isogeny $\eta^\vee : E' \to E$. Then the two points of order 6 in $\ker \eta^\vee$ are

$$\pm\check{P} = \left(-2d^2 + 4d - 1,\ d^3 - \frac{1}{2}d^2 - 2d + \frac{1}{2} \pm \frac{1}{2}(d-1)(9d-1)\sqrt{-3}\right).$$

The point of order 2 in $\ker \eta^\vee$ is

$$3\check{P} = \left(\frac{19}{4}d^2 - \frac{14}{4}d - \frac{1}{4},\ -\frac{19}{8}d^3 - \frac{1}{8}d^2 + \frac{11}{8}d + \frac{1}{8}\right)$$

and the two points of order 3 are

$$\pm 2\check{P} = \left(-2d^2 - 2d - \frac{1}{3},\ d^3 + \frac{5}{2}d^2 + \frac{2}{3}d + \frac{1}{6} \pm \frac{1}{18}(9d-1)^2\sqrt{-3}\right).$$

The number field $\mathbb{Q}(\boldsymbol{\mu}_3) = \mathbb{Q}(\sqrt{-3})$ has degree 2 and class number 1 and the only prime that ramifies is 3. As η is cyclic of degree 6, E also possesses a cyclic isogeny of degree 2 whose kernel is generated by $3P$ and which we denote by $\eta_{\ell=2} : E \to E'_{\ell=2}$, and E possesses a cyclic isogeny of degree 3 whose kernel is generated by $2P$ and which we denote by $\eta_{\ell=3} : E \to E'_{\ell=3}$. Using Vélu's algorithm [Vél71] one easily computes that

$$E'_{\ell=2} : Y^2 + (d+1)XY - d(d-1)Y = X^3 - d(d-1)X^2 - 5d^3X + (3d^2 + d - 1)d^3$$

$$\Delta'_{\ell=2} = d^3(9d-1)^2(d-1)^6.$$

Before we give the explicit examples of $\#Ш(B/\mathbb{Q}) = k \cdot \square$, for $k = 1, 2, 3, 6$, we provide two lemmas. The first one to compute the torsion quotient and the second one to compute the reduction type of E at p and further data.

Lemma 3.4.1. *Let $E/\mathbb{Q}$ be an elliptic curves with a rational 6-torsion point $P = (0,0)$ corresponding to the parameter $d \in \mathbb{Q} \setminus \{0, 1, 1/9\}$ as given above. Assume that $E(\mathbb{Q})_{\text{tors}} = \langle P \rangle \cong \mathbb{Z}/6\mathbb{Z}$ and $E'(\mathbb{Q})_{\text{tors}} = \langle 3\check{P} \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Then*

(i) $\operatorname{coker} \eta^\vee_{\mathbb{Q},\text{tors}}$ can be identified with $\langle d \rangle \times \langle d^2(d-1) \rangle$ in $\mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*3}$, and

(ii) $\operatorname{coker} \eta_{\mathbb{Q},\text{tors}}$ can be identified with $\langle (9d-1)(d-1) \rangle$ in $\mathbb{Q}(\boldsymbol{\mu}_3)^*/\mathbb{Q}(\boldsymbol{\mu}_3)^{*2}$.

Proof. By Remark 2.4.15, we have that $\operatorname{coker} \eta^\vee_{\mathbb{Q},\text{tors}} = \operatorname{coker} \eta^\vee_{\ell=2,\mathbb{Q},\text{tors}} \times \operatorname{coker} \eta^\vee_{\ell=3,\mathbb{Q},\text{tors}}$ and $\operatorname{coker} \eta_{\mathbb{Q},\text{tors}} = \operatorname{coker} \eta_{\ell=2,\mathbb{Q},\text{tors}} \times \operatorname{coker} \eta_{\ell=3,\mathbb{Q},\text{tors}}$. Let $f_2 := X + d$ and $f_3 := Y + 2dX - d^2(d-1)$ be two functions in the function field of $E/\mathbb{Q}$. Then $\operatorname{div}(f_2) = 2(3P) - 2(\mathcal{O})$ and $\operatorname{div}(f_3) = 3(2P) - 3(\mathcal{O})$. Using Proposition 3.2.1, one easily checks that the

embeddings

$$\operatorname{coker}\eta^{\vee}_{\ell=2,\mathbb{Q},\mathrm{tors}} \hookrightarrow H^1(\mathbb{Q}, E'[\eta^{\vee}_{\ell=2}]) \cong \mathbb{Q}^*/\mathbb{Q}^{*2}$$
$$\operatorname{coker}\eta^{\vee}_{\ell=3,\mathbb{Q},\mathrm{tors}} \hookrightarrow H^1(\mathbb{Q}, E'[\eta^{\vee}_{\ell=3}]) \cong \mathbb{Q}^*/\mathbb{Q}^{*3}$$

are given by f_2, respectively f_3. As $f_2(P) \equiv d \bmod \mathbb{Q}^{*2}$, $f_3(P) \equiv d^2(d-1) \bmod \mathbb{Q}^{*3}$, $3P$ generates $\operatorname{coker}\eta^{\vee}_{\ell=2,\mathbb{Q},\mathrm{tors}}$, and $2P$ generates $\operatorname{coker}\eta^{\vee}_{\ell=3,\mathbb{Q},\mathrm{tors}}$, we get (i).

For (ii) note, that by assumption on the torsion groups of E and E', we get that $\operatorname{coker}\eta_{\ell=3,\mathbb{Q},\mathrm{tors}}$ is trivial. For $\operatorname{coker}\eta_{\ell=2,\mathbb{Q},\mathrm{tors}}$ we have to work in the field extension $\mathbb{Q}(\boldsymbol{\mu}_3)$ making the action of Galois on $\ker\eta^{\vee}_{\ell=2}$ trivial. Thus, we only need to compute the embedding

$$\operatorname{coker}\eta_{\ell=2,\mathbb{Q},\mathrm{tors}} \hookrightarrow H^1(\mathbb{Q}(\boldsymbol{\mu}_3), E[\eta_{\ell=2}]) \cong \mathbb{Q}(\boldsymbol{\mu}_3)^*/\mathbb{Q}(\boldsymbol{\mu}_3)^{*2}.$$

Setting $f_2^{\vee} := X - 19/4d^2 + 14/4d + 1/4$, we have $\operatorname{div}(f_2^{\vee}) = 2(3\check{P}) - 2(\mathcal{O})$. From $f_2^{\vee}(\check{P}) = -3/4(d-1)(9d-1)$ we get $f_2^{\vee}(3\check{P}) \equiv (d-1)(9d-1) \bmod \mathbb{Q}(\boldsymbol{\mu}_3)^{*2}$. As $3\check{P}$ generates $\operatorname{coker}\eta_{\ell=2,\mathbb{Q},\mathrm{tors}}$, part (ii) follows. □

Lemma 3.4.2. *Let $E/\mathbb{Q}$ be an elliptic curves with a rational 6-torsion point $P = (0,0)$ corresponding to the parameter $d = u/v \in \mathbb{Q} \setminus \{0, 1, 1/9\}$, with $u, v \in \mathbb{Z}$ coprime. Let p be a prime number.*

(i) If $p|u$ then $\ker\eta_{\ell=2,p} \nsubseteq E_0(\mathbb{Q}_p)$ and $\ker\eta_{\ell=3,p} \nsubseteq E_0(\mathbb{Q}_p)$ and E has split multiplicative reduction at p.

(ii) If $p|u-v$ then $\ker\eta_{\ell=2,p} \subseteq E_0(\mathbb{Q}_p)$ and $\ker\eta_{\ell=3,p} \nsubseteq E_0(\mathbb{Q}_p)$. Further, if $p \neq 2$ then E has split multiplicative reduction at p.

(iii) If $p|v$ then $\ker\eta_{\ell=2,p} \nsubseteq E_0(\mathbb{Q}_p)$ and $\ker\eta_{\ell=3,p} \subseteq E_0(\mathbb{Q}_p)$. Further, if $p \equiv 1 \bmod 3$ then E has split multiplicative reduction at p, and if $p \equiv 2 \bmod 3$ then E has non-split multiplicative reduction at p with

$$c(E'_{\ell=2})_p/c(E)_p = \begin{cases} 1/2, & v_p(v) \text{ odd} \\ 2/2, & v_p(v) \text{ even}. \end{cases}$$

(iii) If $p|9u-v$, $p \neq 2$, and $p \neq 3$ then $\ker\eta_{\ell=2,p} \subseteq E_0(\mathbb{Q}_p)$ and $\ker\eta_{\ell=3,p} \subseteq E_0(\mathbb{Q}_p)$. Further, if $p \equiv 1 \bmod 3$ then E has split multiplicative reduction at p, and if $p \equiv 2 \bmod 3$ then E has non-split multiplicative reduction at p with

$$c(E'_{\ell=2})_p/c(E)_p = \begin{cases} 2/1, & v_p(v) \text{ odd} \\ 2/2, & v_p(v) \text{ even}. \end{cases}$$

Proof. This is an easy exercise and we shortly sketch the proof. First one checks whether $3P$ and $2P$ reduce to a non-singular or singular point to deduce whether $\ker\eta_{\ell=2,p}$ and $\ker\eta_{\ell=3,p}$ lie on $E_0(\mathbb{Q}_p)$. For most of the statements of the lemma one can proceed as in the proof of Lemma 3.3.1. The statement about the Tamagawa quotient follows from Tate's algorithm [Tat75] applied on E and $E'_{\ell=2}$. □

In each of the following four examples we give two parameters $d_1 = u_1/v_1$, and $d_2 = u_2/v_2 \in \mathbb{Q} \setminus \{0, 1, 1/9\}$ that correspond to two elliptic curves E_1 and E_2 over $\mathbb{Q}$ having a rational 6-torsion point. Hence, E_1 and E_2 fulfill Setting 2.4.12 with $N = 6$ and we get $\varphi : E_1 \times E_2 \to B$, with respect to some $n \in (\mathbb{Z}/6\mathbb{Z})^*$. By Corollary 2.4.8, the order of $Ш(B/\mathbb{Q})$ is independent of the choice of n, thus we simply set $n = 1$. Further, we get the corresponding isogenies $\varphi_{\ell=2}$ and $\varphi_{\ell=3}$, which are introduced in Remark 2.4.15. In all four examples, the analytic rank of both elliptic curves E_1 and E_2 is 0 and the discriminant of both curves is negative. Hence, all Tate-Shafarevich groups are finite, the regulator quotient is 1, and the local quotient at infinity for $\varphi_{\ell=2}$ is 1 and for $\varphi_{\ell=3}$ is $1/3$ by Lemma 3.1.1. Also, the rational torsion of E_1 and E_2 is isomorphic to $\mathbb{Z}/6\mathbb{Z}$ and the rational torsion of E_1' and E_2' is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. By construction $\#\ker\varphi_{\mathbb{Q}}/\#\ker\varphi_{\mathbb{Q}}^\vee = 3$. Hence, we can apply Lemma 3.4.1 to compute the torsion quotient. Finally, for both elliptic curves the reduction types at all primes p are 'nice', in the sense that it is possible to apply Theorem 3.1.2. Thus, the local quotients for $\varphi_{\ell=2}$ and $\varphi_{\ell=3}$ are computable for all finite primes p.

Example 3.4.3. ($k = 6$) Choose $d_1 = u_1/v_1 = 2/7$ and $d_2 = u_2/v_2 = 4/17$. Then $\#Ш(B/\mathbb{Q}) = 6\square$.

The Cremona label of E_1 is $770g1$ and of E_2 is $8398i1$. We start with the torsion quotient. By construction, $\#\ker\varphi_{\mathbb{Q}}/\#\ker\varphi_{\mathbb{Q}}^\vee = 3$, and by Lemma 3.4.1, we get

$$\operatorname{coker}\eta_{1,\mathbb{Q},\mathrm{tors}}^\vee = \langle 2\cdot 7\rangle \times \langle 2^2\cdot 5\rangle,\ \operatorname{coker}\eta_{2,\mathbb{Q},\mathrm{tors}}^\vee = \langle 17\rangle \times \langle 2\cdot 13\rangle,$$

$$\operatorname{coker}\eta_{1,\mathbb{Q},\mathrm{tors}} = \langle -5\cdot 11\rangle,\ \operatorname{coker}\eta_{2,\mathbb{Q},\mathrm{tors}} = \langle -13\cdot 19\rangle.$$

From Diagrams (3.1) and (3.2), we conclude that

$$\#\operatorname{coker}\varphi_{\mathbb{Q},\mathrm{tors}}^\vee = 2^2\cdot 3^2 \quad\text{and}\quad \#\operatorname{coker}\varphi_{\mathbb{Q},\mathrm{tors}} = 1.$$

Therefore, the torsion quotient equals $2^2\cdot 3^3$. It remains to calculate the local quotient. The conductor of E_1 is $2\cdot 5\cdot 7\cdot 11$ and of E_2 is $2\cdot 13\cdot 17\cdot 19$. By Lemma 3.1.1, the local quotient at infinity equals 1 if $\ell = 2$, and $1/3$ if $\ell = 3$. From Lemma 3.4.2, we deduce the first two rows of the following table for the finite places p, and with Theorem 3.1.2 we get the third and fourth row. The notation we use is the following. If the reduction type of E_i at p is split multiplicative, then we indicate whether $\ker\eta_{i,\ell=2,p}$ and $\ker\eta_{i,\ell=3,p}$ are contained in $(E_i)_0(\mathbb{Q}_p)$. And if the reduction type of E_i at p is non-split multiplicative, then we give the Tamagawa quotient at p for $\eta_{i,\ell=2}$.

$p =$	2	5	7	11	13	17	19	∞
red. type of E_1	$\notin, \notin$	$\subseteq, \notin$	$\notin, \subseteq$	$\frac{c'}{c} = 2$	good	good	good	
red. type of E_2	$\notin, \notin$	good	good	good	$\subseteq, \notin$	$\frac{c'}{c} = 1/2$	$\subseteq, \subseteq$	
$\frac{\#\operatorname{coker}\varphi_{\ell=2,p}}{\#\ker\varphi_{\ell=2,p}} =$	1/2	1	1/2	1	1	1/2	1	1
$\frac{\#\operatorname{coker}\varphi_{\ell=3,p}}{\#\ker\varphi_{\ell=3,p}} =$	1/3	1/3	1	1	1/3	1	1	1/3

Hence, the local quotient equals $2^{-3} \cdot 3^{-4}$, since by Remark 2.4.15 we get that

$$\#\operatorname{coker} \varphi_p / \#\ker \varphi_p = \#\operatorname{coker} \varphi_{\ell=2,p} / \#\ker \varphi_{\ell=2,p} \cdot \#\operatorname{coker} \varphi_{\ell=3,p} / \#\ker \varphi_{\ell=3,p}.$$

Combining the results, we get $\#Ш(B/\mathbb{Q}) = 6 \cdot \#Ш(E_1 \times E_2/\mathbb{Q}) = 6\square$.

Example 3.4.4. ($k = 3$) Choose $d_1 = 2/7$ and $d_2 = 2/13$. Then $\#Ш(B/\mathbb{Q}) = 3\square$.

The Cremona label of E_1 is $770g1$ and of E_2 is $1430g1$ and the conductor of E_1 is $2 \cdot 5 \cdot 7 \cdot 11$ and of E_2 is $2 \cdot 5 \cdot 11 \cdot 13$. By Lemma 3.4.1, we get

$$\operatorname{coker} \eta^{\vee}_{1,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 7 \rangle \times \langle 2^2 \cdot 5 \rangle,\ \operatorname{coker} \eta^{\vee}_{2,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 13 \rangle \times \langle 2^2 \cdot 11 \rangle,$$

$$\operatorname{coker} \eta_{1,\mathbb{Q},\mathrm{tors}} = \langle -5 \cdot 11 \rangle,\ \operatorname{coker} \eta_{2,\mathbb{Q},\mathrm{tors}} = \langle -5 \cdot 11 \rangle,$$

$$\#\operatorname{coker} \varphi^{\vee}_{\mathbb{Q},\mathrm{tors}} = 2^2 \cdot 3^2 \quad \text{and} \quad \#\operatorname{coker} \varphi_{\mathbb{Q},\mathrm{tors}} = 2.$$

Hence, the torsion quotient equals $2 \cdot 3^3$. The next table follows from Lemma 3.4.2 and Theorem 3.1.2 and implies that the local quotient equals $2 \cdot 3^{-4}$.

$p =$	2	5	7	11	13	∞
red. type of E_1	$\nsubseteq, \nsubseteq$	$\subseteq, \nsubseteq$	$\nsubseteq, \subseteq$	$\frac{c'}{c} = 2$	good	
red. type of E_2	$\nsubseteq, \nsubseteq$	$\frac{c'}{c} = 2$	good	$\subseteq, \nsubseteq$	$\nsubseteq, \subseteq$	
$\frac{\#\operatorname{coker} \varphi_{\ell=2,p}}{\#\ker \varphi_{\ell=2,p}} =$	1/2	2	1/2	2	1/2	1
$\frac{\#\operatorname{coker} \varphi_{\ell=3,p}}{\#\ker \varphi_{\ell=3,p}} =$	1/3	1/3	1	1/3	1	1/3

Therefore, $\#Ш(B/\mathbb{Q}) = 3 \cdot \#Ш(E_1 \times E_2/\mathbb{Q}) = 3\square$.

Example 3.4.5. ($k = 2$) Choose $d_1 = 2/7$ and $d_2 = 6/7$. Then $\#Ш(B/\mathbb{Q}) = 2\square$.

The Cremona label of E_1 is $770g1$ and of E_2 is $1974l1$ and the conductor of E_1 is $2 \cdot 5 \cdot 7 \cdot 11$ and of E_2 is $2 \cdot 3 \cdot 7 \cdot 47$. By Lemma 3.4.1, we get

$$\operatorname{coker} \eta^{\vee}_{1,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 7 \rangle \times \langle 2^2 \cdot 5 \rangle,\ \operatorname{coker} \eta^{\vee}_{2,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 3 \cdot 7 \rangle \times \langle 2 \cdot 3 \rangle,$$

$$\operatorname{coker} \eta_{1,\mathbb{Q},\mathrm{tors}} = \langle -5 \cdot 11 \rangle,\ \operatorname{coker} \eta_{2,\mathbb{Q},\mathrm{tors}} = \langle -47 \rangle,$$

$$\#\operatorname{coker} \varphi^{\vee}_{\mathbb{Q},\mathrm{tors}} = 2^2 \cdot 3^2 \quad \text{and} \quad \#\operatorname{coker} \varphi_{\mathbb{Q},\mathrm{tors}} = 1.$$

Hence, the torsion quotient equals $2^2 \cdot 3^3$. The next table follows from Lemma 3.4.2 and Theorem 3.1.2 and implies that the local quotient equals $2^{-3} \cdot 3^{-3}$.

$p =$	2	3	5	7	11	47	∞
red. type of E_1	$\nsubseteq, \nsubseteq$	good	$\subseteq, \nsubseteq$	$\nsubseteq, \subseteq$	$\frac{c'}{c} = 2$	good	
red. type of E_2	$\nsubseteq, \nsubseteq$	$\nsubseteq, \nsubseteq$	good	$\nsubseteq, \subseteq$	good	$\frac{c'}{c} = 2$	
$\frac{\#\operatorname{coker} \varphi_{\ell=2,p}}{\#\ker \varphi_{\ell=2,p}} =$	1/2	1/2	1	1/2	1	1	1
$\frac{\#\operatorname{coker} \varphi_{\ell=3,p}}{\#\ker \varphi_{\ell=3,p}} =$	1/3	1/3	1/3	3	1	1	1/3

Therefore, $\#Ш(B/\mathbb{Q}) = 2 \cdot \#Ш(E_1 \times E_2/\mathbb{Q}) = 2\square$.

Example 3.4.6. ($k = 1$) Choose $d_1 = 2/7$ and $d_2 = 8/13$. Then $\#Ш(B/\mathbb{Q}) = \square$.

The Cremona label of E_1 is $770g1$ and of E_2 is $7670i1$ and the conductor of E_1 is $2 \cdot 5 \cdot 7 \cdot 11$ and of E_2 is $2 \cdot 5 \cdot 13 \cdot 59$. By Lemma 3.4.1, we get

$$\operatorname{coker} \eta^{\vee}_{1,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 7 \rangle \times \langle 2^2 \cdot 5 \rangle,\ \operatorname{coker} \eta^{\vee}_{2,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 13 \rangle \times \langle 5 \rangle,$$

$$\operatorname{coker} \eta_{1,\mathbb{Q},\mathrm{tors}} = \langle -5 \cdot 11 \rangle,\ \operatorname{coker} \eta_{2,\mathbb{Q},\mathrm{tors}} = \langle -5 \cdot 59 \rangle.$$

$$\#\operatorname{coker} \varphi^{\vee}_{\mathbb{Q},\mathrm{tors}} = 2^2 \cdot 3^2 \quad \text{and} \quad \#\operatorname{coker} \varphi_{\mathbb{Q},\mathrm{tors}} = 1.$$

Hence, the torsion quotient equals $2^2 \cdot 3^3$. The next table follows from Lemma 3.4.2 and Theorem 3.1.2 and implies that the local quotient equals $2^{-2} \cdot 3^{-3}$.

$p =$	2	5	7	11	13	59	∞
red. type of E_1	$\notin, \notin$	$\subseteq, \notin$	$\notin, \subseteq$	$\frac{c'}{c} = 2$	good	good	
red. type of E_2	$\notin, \notin$	$\subseteq, \notin$	good	good	$\notin, \subseteq$	$\frac{c'}{c} = 2$	
$\frac{\#\operatorname{coker} \varphi_{\ell=2,p}}{\#\ker \varphi_{\ell=2,p}} =$	1/2	2	1/2	1	1/2	1	1
$\frac{\#\operatorname{coker} \varphi_{\ell=3,p}}{\#\ker \varphi_{\ell=3,p}} =$	1/3	1/3	1	1	1	1	1/3

Therefore, $\#Ш(B/\mathbb{Q}) = \#Ш(E_1 \times E_2/\mathbb{Q}) = \square$.

Remark 3.4.7. The predicted size of the Tate-Shafarevich group of all occurring elliptic curves E_1 and E_2 is 1. Hence, under this assumption we have provided examples of non-simple non-principally polarised abelian surfaces over $\mathbb{Q}$ such that the order of their Tate-Shafarevich groups are precisely $1, 2, 3, 6$.

3.4.2. $N = 10$

Finally, we give an example for $k = 10$. The elliptic curves over a number field K with a rational 10-torsion point P are given by

$$E : Y^2 + (-d^3 + d^2 + d + 1)XY - d^2(d-1)(d+1)^2 Y = X^3 - d^2(d-1)(d+1)X^2,$$

$$P = (d^3 - d, (d^3 - d)^2),$$

$$\Delta = d^{10}(d-1)^5(d+1)^5(d^2 - 4d - 1)(d^2 + d - 1)^2.$$

Thus if $K = \mathbb{Q}$, then $d \in \mathbb{Q} \setminus \{-1, 0, 1\}$. As usual we denote the isogeny having $\langle P \rangle$ as kernel by $\eta : E \to E'$. The other nine points in the kernel of η are

$$2P = (0, 0),\ 3P = (d^2(d-1)(d+1)^2, -d^4(d-1)(d+1)^2),$$

$$4P = (d^2(d-1)(d+1), d^4(d-1)(d+1)^2),\ 5P = (-d^2, d^4),$$

$$6P = (d^2(d-1)(d+1), 0),\ 7P = (d^2(d-1)(d+1)^2, d^3(d-1)^2(d+1)^3),$$

$$8P = (0, d^2(d-1)(d+1)^2),\ 9P = (d(d-1)(d+1), d(d-1)^2(d+1)).$$

The coefficients a'_1, a'_2, a'_3 for the dual curve E' are the same as for E. The other two coefficients are

$$a'_4 = -5d^{11} - 30d^{10} - 15d^9 + 40d^8 + 65d^7 - 25d^6 - 65d^5 + 40d^4 + 15d^3 - 30d^2 + 5d,$$

$$a'_6 = -d^{17} - 18d^{16} - 56d^{15} - 40d^{14} + 180d^{13} + 151d^{12} - 207d^{11} - 79d^{10} + 65d^9$$
$$-144d^8 + 127d^7 + 221d^6 - 170d^5 - 70d^4 + 61d^3 - 18d^2 + d.$$

Let $\check{P}$ denote a generator of the kernel of the dual isogeny $\eta^\vee : E' \to E$. The point of order 2 in $\ker \eta^\vee$ is

$$5\check{P} = (-1/4 \cdot (d^6 + 14d^5 - 5d^4 - d^2 - 14d + 1),$$

$$-1/8 \cdot (d^9 + 13d^8 - 20d^7 - 10d^6 - 14d^5 - 12d^4 + 20d^3 + 18d^2 + 13d - 1)).$$

As before, E possesses a cyclic isogeny of degree 2 whose kernel is generated by $5P$ and which we denote by $\eta_{\ell=2} : E \to E'_{\ell=2}$, and E possesses a cyclic isogeny of degree 5 whose kernel is generated by $2P$ and which we denote by $\eta_{\ell=5} : E \to E'_{\ell=5}$. Using Vélu's algorithm [Vél71] one easily computes that

$$E'_{\ell=2} : Y^2 + (-d^3 + d^2 + d + 1)XY - d^2(d-1)(d+1)^2Y = X^3 - d^2(d-1)(d+1)X^2$$

$$-5d^5(d^2 + d - 1)X - d^5(d^2 + d - 1)(d^6 - 2d^5 - 5d^4 + 2d + 1),$$
$$\Delta'_{\ell=2} = d^5(d-1)^{10}(d+1)^{10}(d^2 - 4d - 1)^2(d^2 + d - 1).$$

Before presenting the explicit example for $k = 10$, we provide two lemma. The first one to compute the torsion quotient and the second one to compute the reduction type of E at p and further data. The Galois extension $\mathbb{Q}(\boldsymbol{\mu}_5)$ has degree 4 and class number 1 and the only prime that ramifies is 5.

Lemma 3.4.8. *Let $E/\mathbb{Q}$ be an elliptic curves with a rational 10-torsion point $P = (d^3 - d, (d^3 - d)^2)$ corresponding to the parameter $d \in \mathbb{Q} \setminus \{-1, 0, 1\}$ as above. Assume that $E'(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$. Then*

(i) $\operatorname{coker} \eta^\vee_{\mathbb{Q},\text{tors}}$ *can be identified with* $\langle d(d^2 + d - 1)\rangle \times \langle d^4(d-1)(d+1)^3\rangle$ *in* $\mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*5}$, *and*

(ii) $\operatorname{coker} \eta_{\mathbb{Q},\text{tors}}$ *can be identified with* $\langle (d-1)(d+1)(d^2 - 4d - 1)\rangle$ *in* $\mathbb{Q}(\boldsymbol{\mu}_5)^*/\mathbb{Q}(\boldsymbol{\mu}_5)^{*2}$.

Proof. Let $f_2 := X + d^2$ and $f_5 := XY^2/(Y + (d+1)X - (d^5 + d^4 - d^3 - d^2))$ be two functions in the function field of E. Then $\operatorname{div}(f_2) = 2(5P) - 2(\mathcal{O})$ and $\operatorname{div}(f_5) = 5(2P) - 5(\mathcal{O})$. Proceed as in Lemma 3.4.1 and apply Proposition 3.2.1. As $f_2(P) \equiv d(d^2 + d - 1) \bmod \mathbb{Q}^{*2}$ and $f_5(P) \equiv d^4(d-1)(d+1)^3 \bmod \mathbb{Q}^{*5}$ and P generates $\operatorname{coker} \eta^\vee_{\mathbb{Q},\text{tors}}$ we get (i).

For part (ii), we get $\operatorname{coker} \eta_{\ell=5,\mathbb{Q},\text{tors}} = 0$, by assumption on the torsion groups of E and E'. For $\operatorname{coker} \eta_{\ell=2,\mathbb{Q},\text{tors}}$ we have to work in the field extension $\mathbb{Q}(\boldsymbol{\mu}_5)$ making the

action of Galois on $\ker \eta^\vee_{\ell=2}$ trivial. Thus, we only need to compute the embedding

$$\operatorname{coker} \eta_{\ell=2,\mathbb{Q},\mathrm{tors}} \hookrightarrow H^1(\mathbb{Q}(\boldsymbol{\mu}_5), E[\eta_{\ell=2}]) \cong \mathbb{Q}(\boldsymbol{\mu}_5)^*/\mathbb{Q}(\boldsymbol{\mu}_5)^{*2}.$$

The map is given by $f_2^\vee := X + 1/4 \cdot (d^6 + 14d^5 - 5d^4 - d^2 - 14d + 1)$, as $\operatorname{div}(f_2^\vee) = 2(5\check{P}) - 2(\mathcal{O})$. Two of the four points of order 10 in $\ker \eta^\vee$ have X-coordinate equal to

$$(\xi^3 + \xi^2 - 1)d^6 + (-3\xi^3 - 3\xi^2)d^5 + (-7\xi^3 - 7\xi^2 - 1)d^4 + (6\xi^3 + 6\xi^2 + 3)d^3$$

$$+(7\xi^3 + 7\xi^2 + 5)d^2 + (-3\xi^3 - 3\xi^2 - 3)d + (-\xi^3 - \xi^2 - 2),$$

where $\xi \in \boldsymbol{\mu}_5$ is a primitive fifth root of unity. It follows that $f_2^\vee(5\check{P}) \equiv (d-1) \cdot (d+1)(d^2 - 4d - 1) \bmod \mathbb{Q}(\boldsymbol{\mu}_5)^{*2}$. As $5\check{P}$ generates $\operatorname{coker} \eta_{\ell=2,\mathbb{Q},\mathrm{tors}}$ we get (ii). □

Lemma 3.4.9. *Let $E/\mathbb{Q}$ be an elliptic curves with a rational 10-torsion point $P = (d^3 - d, (d^3 - d)^2)$ corresponding to the parameter $d = u/v \in \mathbb{Q} \setminus \{0, 1, 1/9\}$, with $u, v \in \mathbb{Z}$ coprime. Let p be a prime number.*

(i) If $p|uv$ then $\ker \eta_{\ell=2,p} \nsubseteq E_0(\mathbb{Q}_p)$ and $\ker \eta_{\ell=5,p} \nsubseteq E_0(\mathbb{Q}_p)$ and E has split multiplicative reduction at p.

(ii) If $p|(u-v)(u+v)$ then $\ker \eta_{\ell=2,p} \subseteq E_0(\mathbb{Q}_p)$ and $\ker \eta_{\ell=5,p} \nsubseteq E_0(\mathbb{Q}_p)$. Further, if $p \neq 2$ then E has split multiplicative reduction at p.

(iii) If $p|u^2 + uv - v^2$ then $\ker \eta_{\ell=2,p} \nsubseteq E_0(\mathbb{Q}_p)$ and $\ker \eta_{\ell=5,p} \subseteq E_0(\mathbb{Q}_p)$. Further, for $p \neq 5$, if $uv - 2v^2$ is a quadratic residue modulo p then E has split multiplicative reduction at p, and if $uv - 2v^2$ is a quadratic non-residue modulo p then E has non-split multiplicative reduction at p with

$$c(E'_{\ell=2})_p / c(E)_p = \begin{cases} 1/2, & v_p(u^2 + uv - v^2) \text{ odd} \\ 2/2, & v_p(u^2 + uv - v^2) \text{ even}. \end{cases}$$

(iii) If $p|u^2 - 4uv - v^2$ then $\ker \eta_{\ell=2,p} \subseteq E_0(\mathbb{Q}_p)$ and $\ker \eta_{\ell=5,p} \subseteq E_0(\mathbb{Q}_p)$.

Proof. Computing the partial derivatives of the equation for E, one sees that $5P$ reduces to a singular point if and only if $-u^5v^5(u^2 + uv - v^2) \equiv 0 \bmod p$, and that $2P$ reduces to a singular point if and only if $-u^2v^2(u-v)(u+v) \equiv 0 \bmod p$. This determines whether $\ker \eta_{\ell=2,p}$ and $\ker \eta_{\ell=5,p}$ lie on $E_0(\mathbb{Q}_p)$. The remaining statements follow by a case-by-case study using Tate's algorithm [Tat75]. □

Now we give an unconditional example of a non-simple abelian surface B over $\mathbb{Q}$, such that $\#Ш(B/\mathbb{Q}) = 10\square$. As in all the examples of $N = 6$, both elliptic curves have analytic rank equal to 0, hence we can avoid computing the regulator quotient and get the finiteness of the Tate-Shafarevich groups. The local quotient at infinity equals 1 for $\varphi_{\ell=2}$, and $1/5$ for $\varphi_{\ell=5}$. This is due to Lemma 3.1.1, as E_1 and E_2 have negative discriminant. Further, $E_1'(\mathbb{Q})_{\mathrm{tors}} \cong E_2'(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z}$, hence we can use Lemma 3.4.8 to compute the torsion quotient.

Example 3.4.10. ($k = 10$) Choose $d_1 = 5/2$ and $d_2 = 8/5$. Then $\#Ш(B/\mathbb{Q}) = 10\square$.

The Cremona label of E_1 is 123690*by*1 and the conductor of E_2 is 338910. By Lemma 3.4.8, we get

$$\operatorname{coker} \eta^{\vee}_{1,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 5 \cdot 31 \rangle \times \langle 2^2 \cdot 3 \cdot 5^4 \cdot 7^3 \rangle,$$

$$\operatorname{coker} \eta^{\vee}_{2,\mathbb{Q},\mathrm{tors}} = \langle 2 \cdot 5 \cdot 79 \rangle \times \langle 2^2 \cdot 3 \cdot 5^2 \cdot 13^2 \rangle,$$

$$\operatorname{coker} \eta_{1,\mathbb{Q},\mathrm{tors}} = \langle -3 \cdot 7 \cdot 19 \rangle, \ \operatorname{coker} \eta_{2,\mathbb{Q},\mathrm{tors}} = \langle -3 \cdot 13 \rangle.$$

We conclude that

$$\#\operatorname{coker} \varphi^{\vee}_{\mathbb{Q},\mathrm{tors}} = 2^2 \cdot 5^2 \quad \text{and} \quad \#\operatorname{coker} \varphi_{\mathbb{Q},\mathrm{tors}} = 1.$$

By construction, $\#\ker \varphi_{\mathbb{Q}} / \#\ker \varphi^{\vee}_{\mathbb{Q}} = 3$, thus the torsion quotient equals $2^2 \cdot 5^3$. The conductor of E_1 is $2 \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 31$ and of E_2 is $2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 79$. For the primes 11 and 19 we use the equations of E_1, $E'_{1,\ell=2}$, and E_2 to determine that the reduction type of E_1 at $p = 19$ is non-split multiplicative with $c(E'_{1,\ell=2})_p / c(E_1)_p = 2$, and that the reduction type of E_2 at $p = 11$ is split multiplicative. This can be done for example with Sage. The rest of the following table can be read off from Lemma 3.4.9 together with Theorem 3.1.2. Using Remark 2.4.15, it follows that the local quotient equals $2^{-3} \cdot 5^{-6}$.

$p =$	2	3	5	7	11	13	19	31	79	∞
red. type of E_1	$\notin, \notin$	$\subseteq, \notin$	$\notin, \notin$	$\subseteq, \notin$	good	good	$\frac{c'}{c} = 2$	$\notin, \subseteq$	good	
red. type of E_2	$\notin, \notin$	$\subseteq, \notin$	$\notin, \notin$	good	$\subseteq, \subseteq$	$\subseteq, \notin$	good	good	$\frac{c'}{c} = 1/2$	
$\frac{\#\operatorname{coker} \varphi_{\ell=2,p}}{\#\ker \varphi_{\ell=2,p}} =$	1/2	2	1/2	1	1	1	1	1/2	1/2	1
$\frac{\#\operatorname{coker} \varphi_{\ell=3,p}}{\#\ker \varphi_{\ell=3,p}} =$	1/5	1/5	1/5	1/5	1	1/5	1	1	1	1/5

Therefore, we conclude that $\#Ш(B/\mathbb{Q}) = 2 \cdot 5^3 \cdot \#Ш(E_1 \times E_2/\mathbb{Q}) = 10\square$.

Chapter 4.

4 Density questions about non-square order Tate-Shafarevich groups and numerical results

The construction presented in Setting 2.4.12 with $N = 5$ leads to an infinite family of abelian surfaces $B/\mathbb{Q}$, such that the order of $Ш(B/\mathbb{Q})$ is either a square or five times a square, provided it is finite. As this family of abelian surfaces is parametrised by two rational numbers d_1 and d_2, it is possible to sort the family in two natural ways. Firstly, by the *height* of the elliptic curves E_{d_i}, i.e. by the maximum of the absolute value of the numerator and denominator of the d_i, and secondly by the elliptic curves' conductors. Having an ordering of the abelian surfaces, we can ask the following density question: *What is the density of abelian surfaces having Tate-Shafarevich group of order five times a square with respect to the chosen ordering, provided the density exists?*

The results of the previous chapter enable us to determine whether $\#Ш(B/\mathbb{Q})$ is a square or five times a square as long as Mordell-Weil bases for the four corresponding elliptic curves E_{d_1}, E_{d_2}, E'_{d_1}, and E'_{d_2} are known. In the first section of this chapter, we explain how to implement the theorems from the last chapter as an algorithm using computer software. In the second section, we present the numerical results obtained from our calculations. We were able to compute the Tate-Shafarevich groups of the first 18.5 million surfaces in our family with respect to the ordering by height and of the first 2.4 million surfaces with respect to the conductor. As it seems, the density of abelian surfaces having non-square order Tate-Shafarevich groups, if it exists, is about 50% for both orderings. The main results of this chapter are contained in [KK13].

4.1. Algorithm

As seen in Section 3.3.1, every elliptic curve over $\mathbb{Q}$ with a $\mathbb{Q}$-rational 5-torsion point P has a Weierstraß equation

$$E_d : Y^2 + (d+1)XY + dY = X^3 + dX^2,\ P_d = (0,0),$$

for $d \in \mathbb{Q} \setminus \{0\}$. It is easy to check that changing the marked point P results in either the same elliptic curve (E_d, P) or in the elliptic curve given by $-1/d$. Define

$$B_{d_1,d_2} := E_{d_1} \times E_{d_2} / \langle (P_{d_1}, P_{d_2}) \rangle,$$

together with the isogeny $\varphi : E_{d_1} \times E_{d_2} \to B_{d_1,d_2}$. Thus $B_{d_1,d_2}/\mathbb{Q}$ is the abelian surface obtained from Setting 2.4.12 with $n = 1$. Replacing $n = 1$ with either $n = 2$ or with $n = 3$ is the same as replacing one of the d_i with $-1/d_i$. Choosing $n = 4$ results in the same abelian surface and clearly B_{d_1,d_2} is the same surface as $B_{-1/d_1,-1/d_2}$. Since the choice of n does not affect the order of $Ш(B/\mathbb{Q})$ by Corollary 2.4.8, we deduce that to determine the density of abelian surfaces obtained from Setting 2.4.12 with $N = 5$, it is sufficient to consider abelian surfaces B_{d_1,d_2} for d_1 and d_2 being positive. Thus, all elliptic curves E_d can be described by two coprime positive integers (u, v), with $d = u/v$, and we always have $n = 1$. With the same argument, one concludes that it is sufficient to consider only one of the two pairs (d_1, d_2) and (d_2, d_1), thus we only consider unordered pairs $\{d_1, d_2\}$. Finally, if $d_1 = d_2$, then by Corollary 2.4.16 the order of $Ш(B_{d_1,d_2}/\mathbb{Q})$ is always a square. As these abelian surfaces have density zero among all surfaces, we simply omit them in the calculations.

The computation of the local quotient of the Cassels-Tate equation (2.1) is straight forward. From Theorem 3.3.3 it follows, that for each elliptic curve E_d, we essentially only have to know the primes dividing u, v, and $u^2 + 11uv - v^2$. To compute the global quotient we use the identification of $\operatorname{coker} \varphi^\vee_{\mathbb{Q}}$ and $\operatorname{coker} \varphi_{\mathbb{Q}}$ as a subset of $\mathbb{Q}^*/\mathbb{Q}^{*5}$, respectively of $\mathbb{Q}(\boldsymbol{\mu}_5)^*/\mathbb{Q}(\boldsymbol{\mu}_5)^{*5}$. Now assume that we know generators of the Mordell-Weil groups $E_{d_1}(\mathbb{Q})$, $E_{d_2}(\mathbb{Q})$, $E'_{d_1}(\mathbb{Q})$, and $E'_{d_2}(\mathbb{Q})$. Denote by $\eta_{d_i} : E_{d_i} \to E'_{d_i}$ the usual isogeny, and let S_d be the set of all primes p dividing five times the minimal discriminant of E_d, i.e. $p \mid 5uv(u^2 + 11uv - v^2)$. From Proposition 3.2.1 it follows that the image of $\operatorname{coker} \eta^\vee_{d,\mathbb{Q}}$ in $\mathbb{Q}^*/\mathbb{Q}^{*5}$ actually lies in

$$\mathbb{Q}(S_d, 5) := \{x \in \mathbb{Q}^*/\mathbb{Q}^{*5} \mid \ v_p(x) \equiv 0 \bmod 5, \ \forall p \notin S_d\}.$$

Hence, we can represent an element of $\operatorname{coker} \eta^\vee_{d,\mathbb{Q}}$ by its valuation at each prime number $p \in S_d$. The map f_P, which defines the embedding $\operatorname{coker} \eta^\vee_{d,\mathbb{Q}} \hookrightarrow \mathbb{Q}(S_d, 5)$, is computed in Proposition 3.3.4. Once the images of the cokernels of both $\eta^\vee_{d_i,\mathbb{Q}}$ are established, the size of $\operatorname{coker} \varphi^\vee_{\mathbb{Q}}$ can be computed easily by applying the map $(x, y) \mapsto x/y$ on the image of $\operatorname{coker} \eta^\vee_{d_1,\mathbb{Q}} \times \operatorname{coker} \eta^\vee_{d_2,\mathbb{Q}}$, see Section 3.2.

To compute the size of $\operatorname{coker} \varphi_{\mathbb{Q}}$ we represent $\operatorname{coker} \eta_{d,\mathbb{Q}}$ as a subset of

$$\mathbb{Q}(\boldsymbol{\mu}_5)(S_d, 5) := \{x \in \mathbb{Q}(\boldsymbol{\mu}_5)^*/\mathbb{Q}(\boldsymbol{\mu}_5)^{*5} \mid \ v_{\mathfrak{p}}(x) \equiv 0 \bmod 5, \ \forall \mathfrak{p} \notin S_d\},$$

where by $\mathfrak{p} \notin S_d$ we mean a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, such that $\mathfrak{p}$ does not lie above a prime p contained in S_d. The class number of $\mathbb{Q}(\boldsymbol{\mu}_5)$ equals 1, hence to represent elements of $\operatorname{coker} \eta_{d,\mathbb{Q}}$ in $\mathbb{Q}(\boldsymbol{\mu}_5)(S_d, 5)$, we have to fix a generator $t_{\mathfrak{p}}$ for each prime $\mathfrak{p} \in S_d$, and we have to fix generators for the unit group of $\mathbb{Q}(\boldsymbol{\mu}_5)$ modulo fifth powers. The field $\mathbb{Q}(\boldsymbol{\mu}_5)$ is well-known and it is easy to see that the unit group is generated by $-\zeta_5$

and $(1+\zeta_5)$, for ζ_5 a primitive fifth root of unity. Hence,

$$f_{\check{P}}(X,Y) \equiv \zeta_5^{a_0}(1+\zeta_5)^{a_1} \prod_{\mathfrak{p}\in S_d} t_{\mathfrak{p}}^{v_{\mathfrak{p}}(f_{\check{P}}(X,Y))}$$

modulo fifth powers. The map $f_{\check{P}}$ is computed in the discussion after Proposition 3.3.4. To compute the size of coker $\varphi_{\mathbb{Q}}$, determine the order of the kernel of the map$(x,y)\mapsto x/y$, applied on the images of the cokernels of both $\eta_{d_i,\mathbb{Q}}$ in $\mathbb{Q}(\boldsymbol{\mu}_5)(S_{d_i},5)$.

Remark 4.1.1. We can weaken the assumption of having a basis for the Mordell-Weil groups $E_{d_1}(\mathbb{Q}), E_{d_2}(\mathbb{Q}), E'_{d_1}(\mathbb{Q})$ and $E'_{d_2}(\mathbb{Q})$. It is sufficient to just have generators of a finite index sublattice of these four groups, such that the index is not divisible by 5, i.e. the generators of infinite order are not divisible by 5 modulo torsion. Such sublattices suffice because their images in the cokernels of $\eta^{\vee}_{d_i}$, respectively η_{d_i}, are the entire cokernels. Also, it is sufficient to only know such sublattices for $E_{d_1}(\mathbb{Q})$ and $E_{d_2}(\mathbb{Q})$, because suitable dual sublattices can be easily computed using the isogenies η_i. It suffices to calculate the images of the generators under η_{d_i} and then check whether their span contains points divisible by 5 modulo torsion.

The algorithm consists of two main steps and an initialisation step, which we call Step 0. In Step 0, the prime ideal generators $t_{\mathfrak{p}}$ and an ordering of them is fixed. In Step 1, one creates a database $\mathcal{D}$ of elliptic curves having a point P of order 5, which are parametrised by two coprime positive integers (u,v). In Step 2, one takes such a database $\mathcal{D}$ of elliptic curves E_d, for $d=u/v$, and goes over all unordered distinct pairs of these curves and determines whether the order of the Tate-Shafarevich group of the abelian surfaces $B_{d_1,d_2}/\mathbb{Q}$ is a square or a non-square. Optionally, one can use filtering methods to specify which pairs of elliptic curves from $\mathcal{D}$ should be considered. The code is implemented in Sage [S$^+$13] and is available at [Kei12].

Step 0. Creation of a database $\mathcal{F}$ of ordered prime ideal generators $t_{\mathfrak{p}}$.

Input: A positive integer F, which is the prime ideal factorisation bound.

Output: For each prime number $p\leq F$ determine the prime ideals $\mathfrak{p}$ of $\mathbb{Q}(\boldsymbol{\mu}_5)$ above p and fix an ordering of them. Then fix for each prime ideal $\mathfrak{p}$ a generator $t_{\mathfrak{p}}$. Return the ordered generators $t_{\mathfrak{p}}$ in a database $\mathcal{F}$.

Step 1. Creation of a database $\mathcal{D}$ of elliptic curves E_d.

Input: A positive integer H, which is the height bound, and optionally a positive integer C, which is the conductor bound. The database $\mathcal{F}$ from Step 0.

Output: For each pair of coprime positive integers (u,v), such that $\max(u,v)\leq H$, collect the following data

$$\{d, S_d, T_d, U_d, r_d, \mathcal{B}_d^{\vee}, \mathcal{B}_d, \dim \operatorname{coker}\eta_{d,\mathbb{Q}}\}$$

described below associated to the elliptic curve E_d, for $d:=u/v$. Then return this data of all elliptic curves E_d in a database $\mathcal{D}$. Optionally, consider only those pairs (u,v) for which the corresponding elliptic curve E_d has conductor at most C.

(i) Collect all the primes dividing $5uv(u^2+11uv-v^2)$ in a set S_d.

(ii) Collect all the primes dividing uv in a set T_d.

(iii) Collect all the primes $p \equiv 1 \bmod 5$ dividing $u^2+11uv-v^2$ in a set U_d.

(iv) If $v_5(u^2+11uv-v^2)=3$, put also $p=5$ into the set U_d.

(v) Determine the Mordell-Weil rank r_d of E_d.

(vi) Determine a sublattice Λ_d of rank r_d in $E_d(\mathbb{Q})/E_d(\mathbb{Q})_{\text{tors}}$, such that the index is not divisible by 5. Take the image of Λ_d in $\mathbb{Q}(S_d,5)$ to determine a basis $\mathcal{B}_d^\vee$ of $\operatorname{coker}\eta_{d,\mathbb{Q}}^\vee \subset \mathbb{Q}(S_d,5)$. The data for each basis element consists of a pair for each prime in S_d, where the first entry is the corresponding prime in S_d and the second entry is the exponent as an element in $\mathbb{Z}/5\mathbb{Z}$.

(vii) Calculate the image of Λ_d under η_d in $E_d'(\mathbb{Q})$ and determine which image points are divisible by 5 modulo torsion. Divide if possible and determine the non-trivial 5-torsion points of $E_d'(\mathbb{Q})$ to get a sublattice Λ_d' of $E_d'(\mathbb{Q})$, such that the points of infinite order modulo torsion are not divisible by 5. Use this information to get $\dim \operatorname{coker}\eta_{d,\mathbb{Q}}$.

(viii) Take the image of Λ_d' in $\mathbb{Q}(\boldsymbol{\mu}_5)(S_d,5)$ to determine a basis $\mathcal{B}_d$ for $\operatorname{coker}\eta_{\mathbb{Q}} \subset \mathbb{Q}(\boldsymbol{\mu}_5)(S_d,5)$. The data for each basis element consists of a pair for each prime in S_d and a pair for the units. For the primes p in S_d, the first entry is p and the second entry is a list of elements in $\mathbb{Z}/5\mathbb{Z}$, containing as many entries as there are prime ideals $\mathfrak{p}$ in $\mathbb{Q}(\boldsymbol{\mu}_5)$ over p; for the units, the first element is 1 and the second is the list of exponents of the units.

Step 2. Determination of percentage of surfaces B_{d_1,d_2} with non-square order Ш obtained from a filtered database $\mathcal{D}$ of elliptic curves E_d.

Input: A database $\mathcal{D}$ of elliptic curves E_d from Step 1 and the database $\mathcal{F}$ from Step 0. Optionally, some filtering methods which specify which unordered pairs $\{d_1,d_2\}$ of $\mathcal{D}$ are considered.

Output: With respect to the filtering methods, determine the percentage of unordered pairs $\{d_1,d_2\}$ of $\mathcal{D}$ for which the order of $Ш(B_{d_1,d_2}/\mathbb{Q})$ is a non-square. To obtain this percentage do the following for each unordered pair $\{d_1,d_2\}$:

(i) Fix an ordering for $\mathcal{S} := S_{d_1} \cup S_{d_2}$.

(ii) Write out the elements from $\mathcal{B}_{d_1}^\vee \cup \mathcal{B}_{d_2}^\vee$ into a matrix with respect to $\mathcal{S}$. This gives a matrix with entries in $\mathbb{Z}/5\mathbb{Z}$. Calculate the rank of this matrix, which equals the dimension of $\operatorname{coker}\varphi_{\mathbb{Q}}^\vee$.

(iii) Write out the elements from $\mathcal{B}_{d_1} \cup \mathcal{B}_{d_2}$ into a matrix with respect to the prime ideals $(t_{\mathfrak{p}})$ lying over the primes of $\mathcal{S}$ and with respect to the units. This gives a matrix with entries in $\mathbb{Z}/5\mathbb{Z}$. Calculate the rank of this matrix, which equals the dimension of $\operatorname{coker}\psi_{\mathbb{Q}}$.

(iv) $\mathrm{Global}_{d_1,d_2} := \dim \operatorname{coker} \varphi_{\mathbb{Q}}^{\vee} - \dim \operatorname{coker} \eta_{d_1,\mathbb{Q}} - \dim \operatorname{coker} \eta_{d_2,\mathbb{Q}} + \dim \operatorname{coker} \psi_{\mathbb{Q}}$. (Recall that $\dim \operatorname{coker} \varphi_{\mathbb{Q}} = \dim \operatorname{coker} \eta_{d_1,\mathbb{Q}} + \dim \operatorname{coker} \eta_{d_2,\mathbb{Q}} - \operatorname{coker} \psi_{\mathbb{Q}}$.)

(v) $\mathrm{Local}_{d_1,d_2} := -\#(T_{d_1} \cup T_{d_2}) + \#(U_{d_1} \cap U_{d_2})$.

(vi) Return $(\{d_1, d_2\}, \mathrm{Local}_{d_1,d_2} + \mathrm{Global}_{d_1,d_2} \bmod 2)$.

Remark 4.1.2. The final step is justified as follows: The local factor without the infinite prime is a non-square if and only if Local_{d_1,d_2} is odd, and the global factor without the kernels is a non-square if and only if $\mathrm{Global}_{d_1,d_2}$ is odd. Since the contributions of the infinite prime and the kernels cancel, we have that $Ш(B_{d_1,d_2}/\mathbb{Q})$ has non-square order if and only if $\mathrm{Local}_{d_1,d_2} + \mathrm{Global}_{d_1,d_2}$ is odd.

The constructed databases and obtained results are given in the next section. To conclude this section, we make some comments on the implementation. In the cases we considered, Step 0 is not computationally demanding. For example, on a desktop computer it may take some seconds up to a few minutes to compute all generators for all prime ideals of $\mathbb{Q}(\boldsymbol{\mu}_5)$ lying over all primes up to $F = 500\,000$. Step 2 is also no problem. It consists only of simple set operations and calculating ranks of small matrices with coefficients in $\mathbb{Z}/5\mathbb{Z}$. Even a few million of pairs of elliptic curves can be considered in under an hour.

The computational demanding part is Step 1. There are two main issues. The most problematic calculation is to determine the Mordell-Weil rank r and to find r generators of a finite index subgroup of the Mordell-Weil group. To speed up the algorithm we first computed the analytic rank. Then we used the standard Sage method `E.point_search(height_limit=18,rank_bound=r)`, and in case this did not come up with enough points we tried the remaining curves with `E.gens()`. In several cases, these methods did not provide an answer within 48 hours on a single CPU for a single elliptic curve. For these curves we used the method `MordellWeilShaInformation()` in Magma [BCP97], which could handle all our problematic curves in a few seconds each. It is worth noticing, that the method `MordellWeilShaInformation()` can easily determine the Mordell-Weil rank and generators of the Mordell-Weil group for all elliptic curves in our databases in under an second per curve. We used this to check that the computed analytic ranks actually equal the Mordell-Weil ranks. Thus, this first problem is avoidable if one uses Magma instead of Sage.

The second problematic calculation is computing the image of $\operatorname{coker} \eta_{\mathbb{Q}}$ in $\mathbb{Q}(\boldsymbol{\mu}_5)(S,5)$. We need to factor ideals of $\mathbb{Q}(\boldsymbol{\mu}_5)$, which are generated by elements of possibly very big norm. For example, the curve E_d, for $d = 1/94$, has analytic rank 1 and the numerator and denominator of the image of the point of infinite order in $\mathbb{Q}(\boldsymbol{\mu}_5)(S,5)$ have about 600 digits. Sage was not able to factor the corresponding ideal, but using the further information that the image of $\operatorname{coker} \eta_{d,\mathbb{Q}}$ is trivial, as its dimension is zero, it is possible to skip this factorisation. Changing the algorithm accordingly, all curves we tried worked fine. This problem might be avoided by trying another strategy working

modulo primes. The rest of Step 1 consists mainly of factorisation of integers and of rational polynomials of degree 25 (to divide points by 5), as well as calculating isogenies. All these methods work fine for moderately chosen $d = u/v$. On a desktop computer, one could produce in a few hours a database of a few thousand curves using Sage, and in a much shorter time using Magma.

Remark 4.1.3. Since we computed both the analytic and Mordell-Weil rank of the elliptic curves, which agreed in all cases, we know that the curves with Mordell-Weil rank equal to 0 or 1 have finite Tate-Shafarevich groups. For the elliptic curves of Mordell-Weil rank at least 2, we have to assume that the Tate-Shafarevich group is finite. If this group was infinite, then our algorithm would detect whether $\#\ker\varphi^*/\#\operatorname{coker}\varphi^*$ is a square. Here * is the induced morphism on the Tate-Shafarevich groups.

4.2. Results

Given the above described algorithm, one can produce in short time millions of examples of abelian surfaces $B/\mathbb{Q}$, such that either the order of the Tate-Shafarevich group is a square or five times a square. In case the two elliptic curves are both of Mordell-Weil rank $r \leq 1$, these examples are completely unconditional. We constructed two databases of elliptic curves using Step 1 of the algorithm. The first database consists of all elliptic curves E_d, $d = u/v$, such that u, v are positive integers and $\max(u, v) \leq H = 100$. The second database consists of all elliptic curves, with $\max(u, v) \leq H = 50\,000$, such that the conductor of E_d is bounded by $C = 10^6$.

Database 1 contains 6 087 elliptic curves, all of them having Mordell-Weil rank $r \leq 3$. The database is described in more detail in Table 4.1, where we state for each rank the number of elliptic curves with $\max(u, v) \leq H$, for several values of the height H.

H	$\#E_d$	$\#\{r_d = 0\}$	$\#\{r_d = 1\}$	$\#\{r_d = 2\}$	$\#\{r_d = 3\}$
100	6 087	2 390	3 038	633	26
90	4 959	1 987	2 463	490	19
80	3 931	1 597	1 940	380	14
70	2 987	1 235	1 455	287	10
60	2 203	925	1 074	198	6
50	1 547	660	760	123	4
40	979	412	494	70	3
30	555	245	277	33	-
20	255	130	115	10	-
10	63	40	22	1	-

Table 4.1.: Summary of Database 1. For each height bound H, we give the number of elliptic curves E_d, where $d = u/v > 0$ and $\max(u, v) \leq H$. The final four columns give the number of such curves of Mordell-Weil rank 0, 1, 2, and 3.

Database 2 contains 2 212 elliptic curves, all of them having Mordell-Weil rank $r \leq 2$. It is likely that there are no further elliptic curves of conductor at most $C = 10^6$, which have a $\mathbb{Q}$-rational torsion point of order 5, since there is no such curve with $4\,617 < \max(u, v) \leq H = 50\,000$. The database is described in more detail in Table 4.2, where we state for each Mordell-Weil rank the number of elliptic curves with conductor at most $C = 10^6$ and with $\max(u, v) \leq 50\,000$.

H	$\#E_d, C = 10^6$	$\#\{r_d = 0\}$	$\#\{r_d = 1\}$	$\#\{r_d = 2\}$
50 000	2 212	987	1 109	116
4 617	2 212	987	1 109	116
3 072	2 210	986	1 108	116
2 000	2 200	982	1 102	116
1 000	2 174	963	1 095	116
500	2 088	921	1 052	115
200	1 818	786	929	103
100	1 391	616	697	78
50	845	394	405	46

Table 4.2.: Summary of Database 2. For each height bound H, we give the number of elliptic curves E_d of conductor at most $C = 10^6$, where $d = u/v > 0$ and $\max(u, v) \leq H$. The final three columns give the number of such curves of Mordell-Weil rank 0, 1, and 2.

Database 1 yields 18 522 741 abelian surfaces $B_{d_1,d_2}/\mathbb{Q}$. It turns out that 49.31% of these surfaces have Tate-Shafarevich group of non-square order. Database 2 leads to 2 445 366 abelian surfaces. The percentage of the non-square case is 47.01. The intersection of the two databases consists of 1 391 curves, hence we considered 966 745 surfaces twice. In total this gives 20 001 362 surfaces, of which 49.16% have a Tate-Shafarevich group of non-square order.

We did two different experiments with the two databases. In experiment 1 we investigated how the rank influences the squareness of the Tate-Shafarevich group. We list the result in Table 4.3 for Database 1 and in Table 4.4 for Database 2. The first three, respectively four, entries correspond to pairs (E_{d_1}, E_{d_2}) with same Mordell-Weil rank. The following three, respectively six, lines correspond to pairs with different ranks and the final line corresponds to pairs such that both elliptic curves have rank $r \leq 1$. If we consider abelian surfaces of fixed Mordell-Weil rank at least 4, then the density of the surfaces with square Tate-Shafarevich group seems to be significantly larger than 50%. However the surfaces with rank larger than 2 inside our family are conjectured to have density zero and our databases contain very few such cases. The calculations with curves of Mordell-Weil rank $r \leq 1$ all show that the non-square case happens in about 50% of all cases.

For both experiments, we list how many abelian surfaces B_{d_1,d_2} occur in each of the cases and we state the percentage of the surfaces with square Tate-Shafarevich group.

	$H = 100$		
$\{r_{d_1}, r_{d_2}\}$	$\#B_{d_1,d_2}$	$\%(Ш = \square)$	$\%$ (RE $\equiv$ rk B)
$\{r_{d_1}, r_{d_2}\} = \{0,0\}$	2 854 855	48.598	100.00
$\{r_{d_1}, r_{d_2}\} = \{1,1\}$	4 613 203	48.882	80.91
$\{r_{d_1}, r_{d_2}\} = \{2,2\}$	200 028	73.031	44.03
$\{r_{d_1}, r_{d_2}\} = \{3,3\}$	325	98.154	51.08
$\{r_{d_1}, r_{d_2}\} = \{0,1\}$	7 260 820	51.366	91.02
$\{r_{d_1}, r_{d_2}\} = \{0,2\}$	1 512 870	50.567	71.36
$\{r_{d_1}, r_{d_2}\} = \{0,3\}$	62 140	49.891	52.73
$\{r_{d_1}, r_{d_2}\} = \{1,2\}$	1 923 054	52.717	59.50
$\{r_{d_1}, r_{d_2}\} = \{1,3\}$	78 988	60.632	46.23
$\{r_{d_1}, r_{d_2}\} = \{2,3\}$	16 458	84.470	48.23
$r_{d_1}, r_{d_2} \leq 1$	14 728 878	50.051	89.59

Table 4.3.: Results of experiment 1 for Database 1, the curves E_d with $d > 0$ of height at most 100. For each unordered pair of ranks $\{r_{d_1}, r_{d_2}\}$, we list the number of surfaces B_{d_1,d_2} obtained from elliptic curves in database 1 with those ranks. Then, we give the percentage of these surfaces for which Ш has square order, and the last column gives the percentage for which the exponent of the regulator quotient is congruent modulo 2 to the rank of the surface.

	$C = 10^6,\ H = 50\,000$		
$\{r_{d_1}, r_{d_2}\}$	$\#B_{d_1,d_2}$	$\%(Ш = \square)$	$\%$ (RE $\equiv$ rk B)
$\{r_{d_1}, r_{d_2}\} = \{0,0\}$	486 591	54.041	100.00
$\{r_{d_1}, r_{d_2}\} = \{1,1\}$	614 386	58.614	63.51
$\{r_{d_1}, r_{d_2}\} = \{2,2\}$	6 670	92.039	55.53
$\{r_{d_1}, r_{d_2}\} = \{0,1\}$	1 094 583	46.634	83.44
$\{r_{d_1}, r_{d_2}\} = \{0,2\}$	114 492	52.867	47.96
$\{r_{d_1}, r_{d_2}\} = \{1,2\}$	128 644	74.314	42.48
$r_{d_1}, r_{d_2} \leq 1$	2 195 560	51.628	81.53

Table 4.4.: Results of experiment 1 for Database 2, the curves E_d of conductor at most $C = 10^6$ and with $d > 0$ of height at most 50 000. For each unordered pair of ranks $\{r_{d_1}, r_{d_2}\}$, we list the number of surfaces B_{d_1,d_2} obtained from elliptic curves in database 2 with those ranks. Then, we give the percentage of these surfaces for which Ш has square order, and the last column gives the percentage for which the exponent of the regulator quotient is congruent modulo 2 to the rank of the surface.

H	$\#E_d$	$\#B_{d_1,d_2}$	$\%(Ш = \square)$	$\%\ (\mathrm{RE} \equiv \mathrm{rk}\ B)$
100	6 087	18 522 741	50.694	84.14
90	4 959	12 293 361	50.821	83.66
80	3 931	7 724 415	50.941	83.32
70	2 987	4 459 591	51.235	82.51
60	2 203	2 425 503	51.461	82.00
50	1 547	1 195 831	52.211	80.85
40	979	478 731	52.764	79.92
30	555	153 735	54.157	77.12
20	255	32 385	56.384	77.11
10	63	1 953	67.179	74.04

Table 4.5.: Results of experiment 2 for Database 1. For each value of H, we list the number of elliptic curves E_d with $d > 0$ of height at most H, as well as the number of abelian surfaces B_{d_1,d_2} obtained from pairs of such curves. Then, we give the percentage of these surfaces for which Ш has square order, and in the last column we give the percentage for which the exponent of the regulator quotient is congruent modulo 2 to the rank of the surface.

C	$\#E_d$	$\#B_{d_1,d_2}$	$\%(Ш = \square)$	$\%\ (\mathrm{RE} \equiv \mathrm{rk}\ B)$
1 000 000	2 212	2 445 366	52.990	77.84
800 000	1 966	1 931 595	53.232	77.16
600 000	1 683	1 415 403	53.758	76.06
400 000	1 351	911 925	54.215	75.24
200 000	924	426 426	55.001	73.91
100 000	623	193 753	57.074	74.29
80 000	547	149 331	57.776	74.03
60 000	470	110 215	57.990	72.75
40 000	376	70 500	59.306	73.34
20 000	245	29 890	61.288	71.72
10 000	152	11 476	62.182	72.59
5 000	110	5 995	59.783	71.79
1 000	45	990	65.556	76.77

Table 4.6.: Results of experiment 2 for Database 2. For each value of C, we list the number of elliptic curves E_d having conductor at most C and with $d > 0$ of height at most 50 000, as well as the number of abelian surfaces B_{d_1,d_2} obtained from pairs of such curves. Then, we give the percentage of these surfaces for which Ш has square order, and in the last column we give the percentage for which the exponent of the regulator quotient is congruent modulo 2 to the rank of the surface.

Further, we give the percentage in how many cases the parity of the rank of the abelian surface agrees with the parity of the exponent of the regulator quotient (RE). Recall, that if the rank of one of the elliptic curves is at least 2, then we need to assume the finiteness of the Tate-Shafarevich groups, as stated in Remark 4.1.3.

In experiment 2, we looked at the behaviour of the distribution of square and non-square order Tate-Shafarevich groups for increasing height, respectively conductor, of the elliptic curves. Hence, we filtered Database 1 for different values of height bounds H and Database 2 for different values of conductor bounds C. For low bounds, the non-square case was less likely. When we increased these bounds, this frequency tended to approximately 50%. The results of experiment 2 are given in Table 4.5 for Database 1 and Table 4.6 for Database 2.

It is natural to order elliptic curves via height or via conductor, and it is conjectured that densities obtained with respect to these orderings coincide. For both orderings, the density of non-square order Tate-Shafarevich groups seems to exist and is around 50%. This is in contrast to the results of Poonen and Stoll [PS99], who showed that for Jacobians of genus 2 curves the density of non-square order Tate-Shafarevich groups is about 0.13 and this density tends to zero, as the genus goes to infinity.

We end this chapter by giving some heuristics why we expect the density to be 50%. We expect that for a random pair $(d_1 = u_1/v_1, d_2 = u_2/v_2)$ in $\mathbb{Q}^* \times \mathbb{Q}^*$ the global factor is a square for 50% of the abelian surfaces and that the local factor is also a square for 50% of them. We also expect these distributions to be independent. Using the 18 522 741 pairs obtained from the first database, we get numerical evidence for the independence, as illustrated in the following table.

Database 1	global quotient $= \square$	global quotient $\neq \square$
local quotient $= \square$	26.08%	25.26%
local quotient $\neq \square$	24.04%	24.61%

The exponent of the local quotient equals $-\#(T_{d_1} \cup T_{d_2}) + \#(U_{d_1} \cap U_{d_2})$, hence one could prove the expected densities for the local quotient by showing that the probability that the set $(T_{d_1} \cup T_{d_2})$ has an even number of elements is independent of the probability that the set $(U_{d_1} \cap U_{d_2})$ has an even number of elements. The corresponding numerical results for Database 1 are gathered in the following table.

Database 1	$\#(U_{d_1} \cap U_{d_2}) \equiv 0\ (2)$	$\#(U_{d_1} \cap U_{d_2}) \equiv 1\ (2)$
$\#(T_{d_1} \cup T_{d_2}) \equiv 0\ (2)$	46.71%	1.80%
$\#(T_{d_1} \cup T_{d_2}) \equiv 1\ (2)$	49.55%	1.95%

The global quotient is harder to control. The exponent of the torsion quotient equals 3 on a density 1 subset of the pairs (d_1, d_2), see Proposition 3.3.6. The results of Tables 4.3, 4.4, 4.5, and 4.6 suggest that the squareness of the regular quotient and hence the squareness of the global quotient depends on the parity of the rank. If both ranks of the elliptic curves E_{d_1} and E_{d_2} are equal to 0, hence are even, the regulator quotient equals 1, hence is a square. If one elliptic curve is of rank 0 and the other is of rank 1,

then the regulator quotient is a non-square if and only if $\operatorname{coker} \eta_{\mathbb{Q}}$ is trivial modulo torsion, where η is the usual isogeny belonging to the elliptic curve of rank 1.

In Database 1, we have the following situation. For the rank 1 curves, it happens in about 91.2% of the cases that $\eta_{\mathbb{Q}}$ is surjective on the free part. In case both ranks are equal to 1, the regulator quotient is a square in about 80.9% of the cases. For the complete Database 1, we get that the parity of the exponent of the regulator quotient agrees with the parity of the rank in 84.14%. If we consider only elliptic curves of rank at most 1, then we have that for abelian surfaces B_{d_1,d_2} of even rank the regulator quotient is a square in about 88.2% of the cases. Further, for abelian surfaces B_{d_1,d_2} of odd rank the regulator quotient is a non-square in about 91.0% of the cases, which together gives 89.6% of agreement. We have the following situation for Database 1.

Database 1	$\operatorname{rk}(B_{d_1,d_2}) \equiv 0\ (2)$	$\operatorname{rk}(B_{d_1,d_2}) \equiv 1\ (2)$
regulator quotient $= \square$	42.067%	7.931%
regulator quotient $\neq \square$	7.927%	42.075%

In contrast to the global quotient, the squareness of the local quotient seems to be independent of the parity of the rank of the abelian surfaces. Again we give the numerical results for Database 1.

Database 1	$\operatorname{rk}(B_{d_1,d_2}) \equiv 0\ (2)$	$\operatorname{rk}(B_{d_1,d_2}) \equiv 1\ (2)$
local quotient $= \square$	25.670%	25.675%
local quotient $\neq \square$	24.324%	24.331%

Remark 4.2.1. (i) We also did computations for Setting 2.4.12 with $N = 7$, but on a much smaller scale. The percentages obtained are very similar to the case $N = 5$.

(ii) In the last section of the previous chapter, we have seen that if we consider Setting 2.4.12 with $N = 6$, then it is possible that $\#Ш(B/\mathbb{Q}) = k \cdot \square$, for $k = 1, 2, 3, 6$. It would be interesting to investigate how often these four different values for k do occur while ranging through all pairs of elliptic curves having a rational 6-torsion point, sorted by increasing height or conductor.

(iii) The first curve E_1 is the same curve in all four examples for $N = 6$. Hence, one could ask a related density question about the distribution of the four different values for k while fixing one of the two elliptic curves and varying the other one. Of course one could ask the same question for other values of N.

Chapter 5.

5 Obstructions to non-square order Tate-Shafarevich groups of non-simple abelian surfaces over the rationals

The motivation of this thesis is Question 1.2.4: *What are the possible non-square parts of the orders of finite Tate-Shafarevich groups for abelian varieties of fixed dimension over a fixed number field? Is this a finite list?* We would like to give an answer to this question when we restrict ourselves to the case of non-simple abelian surfaces over the rationals. By Remark 2.4.3, to study the possible non-square parts of the order of Tate-Shafarevich groups of non-simple abelian surfaces B/K over a number field K, it is sufficient to study isogenies $\varphi : E_1/K \times E_2/K \to B$ having diagonal kernel. As seen in Section 2.4, the existence of φ implies that there are isogenies $\eta_i : E_i \to E_i'$ and a Galois equivariant isomorphism $\alpha : \ker \eta_1 \to \ker \eta_2$, such that $\ker \varphi$ equals the graph of α. Hence to some extent, we are reduced to the study of isogenies of elliptic curves. It is a standard fact that isogenies between elliptic curves factor into a product of a cyclic isogeny of degree N and a multiplication-by-n endomorphism $[n]$, for uniquely determined natural numbers N and n.

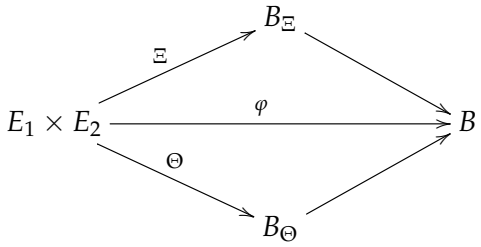
Lemma 5.0.2. *Let $\eta : E \to E'$ be an isogeny between two elliptic curves over a number field K. Then there is a unique $n \in \mathbb{N}$ and a cyclic isogeny $\theta : E \to E'$ of degree $N = \deg \eta / n^2$, such that $\eta = \theta \circ [n]_E = [n]_{E'} \circ \theta$.*

We obtain the following general setting.

Setting 5.0.3. Let E_1 and E_2 be two elliptic curves over a number field K and let $\varphi : E_1 \times E_2 \to B$ be an isogeny with diagonal kernel. Denote by G a finite group scheme over K being isomorphic to $\ker \varphi$. Then there are embeddings $\iota_i : G \hookrightarrow E_i$, such that $\ker \varphi$ is the image of $\iota_1 \times \iota_2$. The image $G_i := \iota_i(G)$ of G in E_i determines an isogeny $\eta_i : E_i \to E_i'$, via $\ker \eta_i := G_i$. Denote by $\alpha : G_1 \to G_2$ the Galois equivariant isomorphism, such that $\alpha \circ \iota_1 = \iota_2$. Hence, $\ker \varphi$ is the graph of α.

By Lemma 5.0.2, the isogenies η_i factor through a cyclic isogeny $\theta_i : E_i \to E_i'$ of degree N and a multiplication-by-n map $[n] : E_i \to E_i$ of degree n^2. The restriction of α

to an isomorphism $\ker\theta_1 \to \ker\theta_2$ determines a cyclic isogeny $\Theta : E_1 \times E_2 \to B_\Theta$ with diagonal kernel of degree N. The same procedure applied on $E_1[n] \to E_2[n]$ gives an isogeny $\Xi : E_1 \times E_2 \to B_\Xi$ with diagonal kernel of degree n^2, which we call the *diagonal multiplication-by-n map*. We obtain the following commutative diagram.



Hence, if $\gcd(N, n) = 1$ and one knows the non-square part of the order of $Ш(B_\Xi/K)$ and of $Ш(B_\Theta/K)$, then one can deduce the non-square part of the order of $Ш(B/K)$. Further, we can conclude that the number of possibilities for the non-square part of the order of $Ш(B/K)$ is finite, if the number of possibilities for the non-square part of the order of $Ш(B_\Xi/K)$, as well as the number of possible primes dividing the degrees of cyclic isogenies between elliptic curves over K, are finite.

In the next section, we recall known facts about quadratic twists of abelian varieties and about cyclic isogenies between elliptic curves over $\mathbb{Q}$. Using these results, we prove in Section 5.2 that in the special case of $K = \mathbb{Q}$, there are only the eight possibilities $\{1, 2, 3, 5, 6, 7, 10, 13\}$ for the non-square part of the order of $Ш(B_\Theta/\mathbb{Q})$ and all eight cases occur, see Theorem 5.2.7. The situation for $Ш(B_\Xi/\mathbb{Q})$ remains unclear. We are not able to answer whether there are only finitely many k, such that $Ш(B_\Xi/\mathbb{Q}) = k \cdot \square$. In Section 5.3 we show, that this list is indeed finite, if one considers all possible diagonal multiplication-by-n maps $\Xi : E_1 \times E_2 \to B_\Xi$, for all n, but E_1 and E_2 belong to a fixed finite set of elliptic curves over $\mathbb{Q}$. This result is given in Corollary 5.3.10. To conditionally improve this result, we present two hypotheses which would imply that there are only finitely many possibilities for the non-square part of the order of $Ш(B_\Xi/\mathbb{Q})$. Hence, as long as one restricts oneself to non-simple abelian surfaces $B/\mathbb{Q}$, then the answer to the second part of Question 1.2.4 is indeed *yes*, provided these hypotheses are true. These conditional results are given in 5.3.13 and 5.3.14. Finally, we show that there is an example with $Ш(B_\Xi/\mathbb{Q}) = 2 \cdot \square$, which also fulfills $Ш(B_\Theta/\mathbb{Q}) = 7 \cdot \square$. Hence, we get a non-simple abelian surface $B/\mathbb{Q}$, such that $Ш(B/\mathbb{Q}) = 14 \cdot \square$; see Example 5.3.23.

5.1. Qudratic twists and cyclic isogenies of elliptic curves over $\mathbb{Q}$

Everything contained in this section is well-known. We fix notation and recall some terminology. Let K denote a field of characteristic 0 and let A be an abelian variety over K. A twist of A is an abelian variety A' over K which is isomorphic to A over $\overline{K}$. Denote by $\kappa_A : A \to A'$ such a $\overline{K}$-isomorphism. As the absolute Galois group Gal_K acts on the set of $\overline{K}$-rational points of A and A', we get induced $\overline{K}$-automorphisms $\epsilon_\sigma : A \to A$

and $\epsilon'_\sigma : A' \to A'$, for each $\sigma \in \mathrm{Gal}_K$. With $\mathrm{Aut}_{\overline{K}}(A/K)$ we denote the group of $\overline{K}$-automorphisms of the abelian variety $(A/K, \mathcal{O})$. For $\kappa \in \mathrm{Aut}_{\overline{K}}(A/K)$, we define $\kappa^\sigma := \epsilon_\sigma \circ \kappa \circ \epsilon_\sigma^{-1}$ to endow $\mathrm{Aut}_{\overline{K}}(A/K)$ with the natural structure of a K-Galois module, see Chapter 2 of [Mil72]. The map $\sigma \mapsto \kappa_A^{-1} \circ \epsilon'_\sigma \circ \kappa_A \circ \epsilon_\sigma^{-1}$ defines a cocycle $\xi : \mathrm{Gal}_K \to \mathrm{Aut}_{\overline{K}}(A/K)$. The cohomology class $[\xi] \in H^1(K, \mathrm{Aut}_{\overline{K}}(A/K))$ is determined by the K-isomorphism class of A'/K and is independent of the choice of κ_A. Further, for each $[\xi] \in H^1(K, \mathrm{Aut}_{\overline{K}}(A/K))$, there is a twist A'/K of A/K giving rise to the cocycle ξ. Hence, the set of twists of A/K (up to K-isomorphism) can be identified with $H^1(K, \mathrm{Aut}_{\overline{K}}(A/K))$. For elliptic curves, this is Proposition X.5.3 of [Sil86].

The possibly non-abelian group $\mathrm{Aut}_{\overline{K}}(A/K)$ contains the subgroup of order 2 generated by the multiplication-by-(-1) automorphism $[-1]$. For a general abelian variety, such as elliptic curves with j-invariant different from 0 and 1728, this is all of $\mathrm{Aut}_{\overline{K}}(A/K)$. As $\langle [-1] \rangle$ embeds into $\mathrm{Aut}_{\overline{K}}(A/K)$, we get the induced map

$$H^1(K, \langle [-1] \rangle) \to H^1(K, \mathrm{Aut}_{\overline{K}}(A/K)).$$

Clearly, this map is injective if $\mathrm{Aut}_{\overline{K}}(A/K) = \mathrm{Aut}_K(A/K)$. By Hilbert 90, there is a unique isomorphism $\delta_K : K^*/K^{*2} \cong H^1(K, \langle [-1] \rangle)$. For each $D \in K^*/K^{*2}$ denote by $\xi_D : \mathrm{Gal}_K \to \langle [-1] \rangle$ the cocycle associated to D via δ_K, thus ξ_D factors through $\mathrm{Gal}(K(\sqrt{D})/K)$. Further, let $\chi_D : \mathrm{Gal}_K \to \{\pm 1\} \subseteq K^*$ be the quadratic character associated to D, hence $\sqrt{D}^\sigma = \chi_D(\sigma) \cdot \sqrt{D}$. Clearly, $\xi_D(\sigma) = [-1]$ if and only if $\chi_D(\sigma) = -1$.

Define A^D/K to be the twist of A/K corresponding to the image of ξ_D in $H^1(K, \mathrm{Aut}_{\overline{K}}(A/K))$. We call A^D/K the *quadratic twist by* $[-1]$ *of* A/K *with respect to* D, or in short the *quadratic twist of* A/K *with respect to* D. The abelian varieties A/K and A^D/K are isomorphic over the field extension $K(\sqrt{D})$. By definition, the cocycle associated to A^D/K equals ξ_D, thus $\xi_D(\sigma) = \kappa_A^{-1} \circ \epsilon_\sigma^D \circ \kappa_A \circ \epsilon_\sigma^{-1}$ and hence

$$\epsilon_\sigma^D = \kappa_A \circ \xi_D(\sigma) \circ \epsilon_\sigma \circ \kappa_A^{-1} \in \mathrm{Aut}_{\overline{K}}(A^D/K).$$

As a direct consequence of the given formula, we deduce the following lemma which describes how quadratic twisting alters the action of Galois on the n-torsion.

Lemma 5.1.1. *Let d be the dimension on A/K. Fix a basis $\mathcal{B}$ for $A[n]$ and denote its image under $\kappa_A : A \to A^D$ by $\mathcal{B}^D$. Let the action of $\sigma \in \mathrm{Gal}_K$ on $A[n]$ with respect to $\mathcal{B}$ be given by the matrix $M(\sigma) \in \mathrm{GL}_{2d}(\mathbb{Z}/n\mathbb{Z})$, and the action on $A^D[n]$ with respect to $\mathcal{B}^D$ be given by the matrix $M^D(\sigma) \in \mathrm{GL}_{2d}(\mathbb{Z}/n\mathbb{Z})$.*

(i) For all $\sigma \in \mathrm{Gal}_K$ we have $M^D(\sigma) = \chi_D(\sigma) \cdot M(\sigma)$.

(ii) The isomorphism $\kappa_A : A \to A^D$ establishes a one-to-one correspondence between finite Galois invariant subgroups of $A(\overline{K})$ and $A^D(\overline{K})$. This correspondence is independent of the choice of κ_A.

Proof. Part (i) is immediate from the above formula and (ii) follows directly from (i). □

Now we define the quadratic twist φ_D of an isogeny $\varphi : A \to B$ between abelian varieties A and B over K. By the second part of the above lemma, the image of the

kernel of φ under the $K(\sqrt{D})$-isomorphism $\kappa_A : A \to A^D$ is a finite Galois equivariant subgroup of A^D, thus it is the kernel of an isogeny, which we denote by φ_D. It is obvious that the codomain of φ_D equals B^D and that there is a $K(\sqrt{D})$-isomorphism $\kappa_B : B \to B^D$ making the following diagram commutative over $K(\sqrt{D})$.

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle \kappa_A}\downarrow & & \downarrow{\scriptstyle \kappa_B} \\ A^D & \xrightarrow[\varphi_D]{} & B^D \end{array}$$

We present two lemmas describing the effect of twisting. The first lemma deals with the fields of definition of kernels of isogenies under twisting.

Lemma 5.1.2. *If φ has a L-kernel, for a field L/K, then φ_D has a $L(\sqrt{D})$-kernel. If further $\sqrt{D} \notin L$ and* $\ker \varphi$ *contains a point of order at least* 3*, then φ_D does not have a L-kernel.*

Proof. The isomorphism κ_A induces an isomorphism between $L(\sqrt{D})$-rational points of A and A^D identifying $\ker \varphi$ with $\ker \varphi_D$, thus φ_D has a $L(\sqrt{D})$-kernel. Now assume that $\sqrt{D} \notin L$ and let σ be the non-trivial element of $\mathrm{Gal}(L(\sqrt{D})/L)$. As seen above, for a point $Q \in A^D(\overline{K})$ the action of Galois is given by $\epsilon_\sigma^D = \kappa_A \circ \xi_D(\sigma) \circ \epsilon_\sigma \circ \kappa_A^{-1}$. Assume that Q lies in the kernel of φ_D, hence $P := \kappa_A^{-1}(Q)$ lies in the kernel of φ, and thus $P \in A(L)$. It follows that ϵ_σ has no effect on P, but $\xi_D(\sigma)$ sends it to $-P$, as $\sqrt{D} \notin L$. Therefore, $\epsilon_\sigma^D(Q) = -Q$, and thus φ_D does not have a L-kernel, if $\ker \varphi$ contains a point of order at least 3. □

The second lemma is concerned with the value of $|\varphi'(0)|_v$ under twisting. We need this lemma for the examples in Appendix A.

Lemma 5.1.3. *Let $\varphi : A \to B$ be an isogeny between abelian varieties over a number field K and let $v \in M_K^0$ be a finite place of K. If $v \nmid D$ and A and B have good reduction at v, then $|\varphi'(0)|_v = |\varphi'_D(0)|_v$.*

Proof. Define the quadratic field extension $L := K(\sqrt{D})$ and let $w \in M_L^0$ be a place lying over v. As $v \nmid D$, we have that L/K is unramified at v. In case of unramified extensions and good reduction we have that Néron models behave well under base change, i.e. the Néron model of A/L is the base change to L of the Néron model of A/K. It follows that that $|\varphi'(0)|_v = |\varphi'(0)|_w$ and $|\varphi'_D(0)|_v = |\varphi'_D(0)|_w$. Further, as A and A^D are isomorphic over L we also get that $|\varphi'(0)|_w = |\varphi'_D(0)|_w$. Therefore, $|\varphi'(0)|_v = |\varphi'_D(0)|_v$. □

For the rest of the section, let A/K be an elliptic curve E/K. If $Y^2 = f(X)$ is a short Weierstrass model for E/K, then $DY^2 = f(X)$ is an equation for E^D/K and $\kappa_E : E \to E^D$ is given by $(X, Y) \mapsto (X, Y/\sqrt{D})$. If E possesses a cyclic N-isogeny, which is equivalent to E having a Galois invariant cyclic subgroup of order N, then there is a basis for $E[N]$ such that the action of Galois looks like $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. In this case a and d are group homomorphisms $\mathrm{Gal}_K \to (\mathbb{Z}/N\mathbb{Z})^*$. If E admits two cyclic N-isogenies φ and ψ, such

that $\ker \varphi_{\overline{K}} \cap \ker \psi_{\overline{K}} = 0$, then there is a basis of $E[N]$ such that the action of Galois looks like $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$. In this case, we say that E possesses *independent* cyclic N-isogenies. Set-theoretically that means, that $E[N]$ has two different Galois invariant cyclic subgroups of order N which generate $E[N]$. In case E possesses a cyclic N-isogeny and this is the only cyclic N-isogeny, then we say E possesses a *unique* cyclic N-isogeny. Set-theoretically that means, that $E[N]$ has precisely one Galois invariant cyclic subgroup of order N. There is a further possibility, in which E possesses two cyclic N-isogenies that are not independent. That means that set-theoretically $E[N]$ has more than one Galois invariant cyclic subgroup of order N, but there is no choice of two of them, such that these two generate all of $E[N]$. In this case, we say that E has *dependent* isogenies.

If $N \geq 2$, then it is clear that the four properties of having no cyclic N-isogeny, of having a unique cyclic N-isogeny, of having independent cyclic N-isogenies, and of having dependent cyclic N-isogenies, are mutually exclusive and cover all possibilities. In the next lemma, we show that the case of dependent cyclic N-isogenies cannot happen for N being prime.

Lemma 5.1.4. *Let E be an elliptic curve over a field K and assume that E admits a cyclic N-isogeny for a positive integer $N \geq 2$.*

(i) If N is prime, then either the isogeny is unique or E has independent cyclic N-isogenies.

(ii) If $N = \prod_i \ell_i^{e_i}$ is composite, with the ℓ_i being pairwise different primes, then

(a) the isogeny is unique if and only if E possesses a unique cyclic $\ell_i^{e_i}$-isogeny, for every prime ℓ_i dividing N.

(b) E has independent cyclic N-isogenies if and only if E has independent cyclic $\ell_i^{e_i}$-isogenies, for every prime ℓ_i dividing N.

Proof. If N is prime, then two different cyclic subgroups of order N always generate all of $E[N]$, which proves (i). The second part of the lemma follows directly from the fact that $E[\ell_i^\infty] \cap E[\ell_j^\infty] = 0$, for $\ell_i \neq \ell_j$. □

There is the following effect of quadratic twisting on elliptic curves.

Lemma 5.1.5. *Let E be an elliptic curve over a field K and E^D a quadratic twist of E.*

(i) If $N \geq 2$, then the four pairwise exclusive properties of an elliptic curve of having no cyclic N-isogeny, of having a unique cyclic N-isogeny, of having independent cyclic N-isogenies, and of having dependent cyclic N-isogenies, are stable under quadratic twisting, i.e. E has one of the properties if and only if E^D has the same property.

(ii) If $N \geq 3$, then twisting changes the isomorphism type of the kernel of a cyclic N-isogeny. Therefore, if an elliptic curve E possesses a unique cyclic N-isogeny, then E and E^D possess cyclic N-isogenies with isomorphic kernels if and only if E and E^D are isomorphic.

Proof. For (i) recall that twisting establishes a one-to-one correspondence between Galois invariant subgroups, by Lemma 5.1.1.

To establish (ii), note that by Lemmas 5.1.1 and 5.1.2 the kernel of a cyclic N-isogeny is isomorphic to the kernel of the corresponding twisted isogeny if and only if $\chi_D \equiv 1$, which is impossible for a non-trivial twist and $N \geq 3$. If the isogenies are unique,

then they correspond to each other under twisting, hence for them to have isomorphic kernels forces the twist to be trivial, thus the elliptic curves are isomorphic. □

There is a variation of the above lemma considering factorisations of division polynomials.

Lemma 5.1.6. *(i) Quadratic twisting preserves the* type of factorisation *of division polynomials, i.e. if $f = \prod f_i$ is a factorisation of the N-division polynomial f of the elliptic curve E/K into irreducible factors f_i, then the N-division polynomial f^D of its quadratic twist E^D/K factors into the same number of irreducible polynomials f_j^D, and there is an ordering of these f_j^D, such that the degree of f_i^D equals the one of f_i.*

(ii) Let E_1 and E_2 be two elliptic curves over a field K having cyclic N-isogenies η_i with isomorphic kernels. Then the kernel polynomials of η_1 and η_2 have the same type of factorisation.

Proof. Let E be an elliptic curve with quadratic twist E^D. Assume they are given by $E : Y^2 = f(X)$ and $E^D : DY^2 = f(X)$. It follows that the X-coordinates of the points in $E[N]$ and those of $E^D[N]$ form the same sets of algebraic numbers. Hence, Galois acts in exactly the same manner on the roots of the N-division polynomial of E and of E^D. The same is true for the roots of the kernel polynomial of η_1 and η_2, as these Galois modules are assumed to be isomorphic. As a monic univariate polynomial over the rationals with pairwise different roots breaks precisely into the irreducible factors under the Galois orbits of its roots, we get the lemma. □

From now on, if E/K is an elliptic curve possessing a cyclic N-isogeny, then we assume that the action of Galois on $E[N]$ is given by $\begin{pmatrix} a & * \\ 0 & d \end{pmatrix}$.

Corollary 5.1.7. *If $N = \ell$ is prime and E/K has at least three different cyclic ℓ-isogenies, i.e. $E[\ell]$ contains at least three different Galois invariant subgroups, then $a(\sigma) \equiv d(\sigma)$.*

Proof. By Lemma 5.1.4, E has independent cyclic ℓ-isogenies, hence the action of Galois on $E[\ell]$ can be given by $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$, with respect to two generators P and Q of $E[\ell]$. Clearly, the cyclic subgroups generated by P, respectively Q, are Galois invariant. As there is a third such group and ℓ is prime, there is a $n_0 \in (\mathbb{Z}/\ell\mathbb{Z})^*$, such that $P + n_0Q$ generates a Galois invariant subgroup. As $(P + n_0Q)^\sigma = a(\sigma)P + n_0d(\sigma)Q$, we deduce that $a(\sigma)P + n_0d(\sigma)Q$ has to be a multiple of $P + n_0Q$, hence $a(\sigma) = d(\sigma)$, for all $\sigma \in \mathrm{Gal}_K$. □

Let $N \geq 2$ be a positive integer and denote by $\chi_N : \mathrm{Gal}_K \to (\mathbb{Z}/N\mathbb{Z})^*$ the mod-N cyclotomic character, i.e. for all $\sigma \in \mathrm{Gal}_K$ we have that if ξ_N is a primitive N-th root of unity and $\xi_N^\sigma = \xi_N^k$, for some $k \in (\mathbb{Z}/N\mathbb{Z})^*$, then $\chi_N(\sigma) = k$. In the next lemma, we recall the fact that the determinant of the mod-N Galois representation of an elliptic curve E/K equals χ_N.

Lemma 5.1.8. *If E/K has a cyclic N-isogeny, then $a(\sigma) \cdot d(\sigma) \equiv \chi_N(\sigma)$.*

Proof. Denote the cyclic N-isogeny by η. Let $e : \ker\eta \times \ker\eta^\vee \to \boldsymbol{\mu}_N \subseteq \overline{K}^*$ denote the Weil pairing with respect to η and its dual $\eta^\vee$. If P is a generator of $\ker\eta$ and $\check{P}$ a

generator of $\ker \eta^\vee$, then $e(P, \check{P}) = \xi_N$, for some primitive N-th root of unity ξ_N. As the action of Galois on a generator of $\ker \eta$ is given by a and its action on a generator on $\ker \eta^\vee$ is given by d, we get

$$\xi_N^{a(\sigma)\cdot d(\sigma)} = e(P, \check{P})^{a(\sigma)\cdot d(\sigma)} = e(a(\sigma)\cdot P, d(\sigma)\cdot \check{P}) = e(P^\sigma, \check{P}^\sigma) = e(P, \check{P})^\sigma = \xi_N^{\chi_N(\sigma)},$$

due to the Galois invariance of the Weil pairing. □

Corollary 5.1.9. *If the mod-N cyclotomic character $\chi_N : \mathrm{Gal}_K \to (\mathbb{Z}/N\mathbb{Z})^*$ is surjective for $N \geq 3$ and E/K has a cyclic N-isogeny η, then $a(\sigma) \not\equiv d(\sigma)$, i.e. $\ker \eta \ncong \ker \eta^\vee$.*

Proof. Assume to the contrary that $a(\sigma) \equiv d(\sigma)$, then $a(\sigma)^2 \equiv \chi_N(\sigma)$, by Lemma 5.1.8. Hence, all values of $\chi_N(\sigma)$ are quadratic residues mod N. The homomorphism $(\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/N\mathbb{Z})^*$, given by $x \mapsto x^2$, is not an isomorphism as $1 \neq -1 \mapsto 1$. Therefore, there are quadratic non-residues mod N in $(\mathbb{Z}/N\mathbb{Z})^*$, contradicting the surjectivity of $\chi_N(\sigma)$. □

We state two nice consequences for elliptic curves over $\mathbb{Q}$.

Corollary 5.1.10. *Assume that $N = \ell \neq 2$ is an odd prime and $K = \mathbb{Q}$.*
(i) An elliptic curve $E/\mathbb{Q}$ cannot have more than two different cyclic ℓ-isogenies.
(ii) If $E/\mathbb{Q}$ possesses a cyclic ℓ-isogeny η, then $a(\sigma) \not\equiv d(\sigma)$, i.e. $\ker \eta \ncong \ker \eta^\vee$.

Proof. The mod-ℓ cyclotomic character $\chi_\ell : \mathrm{Gal}_\mathbb{Q} \to (\mathbb{Z}/\ell\mathbb{Z})^*$ is surjective, as the ℓ-th cyclotomic polynomial is irreducible over $\mathbb{Q}$. Now everything follows directly from Corollaries 5.1.7 and 5.1.9. □

For elliptic curves over $\mathbb{Q}$, the possible cyclic isogenies are completely classified due to Mazur with some remaining gaps filled by Kenku.

Theorem 5.1.11 (Mazur, Kenku)**.** *There is an elliptic curve $E/\mathbb{Q}$ possessing a cyclic isogeny of degree N if and only if N equals one of the 26 values in the following set*

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 25, 27, 37, 43, 67, 163\}.$$

Proof. See [Maz78] and [Ken82]. □

The corresponding modular curve $X_0(N)$ is of genus 0 if and only if N equals one of the 15 values in the following set

$$T := \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\},$$

and $X_0(N)$ is of genus 1 if and only if N equals one of the 12 values in the following set $\{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$. A detailed treatment of the genus 1 case can be found in [Lig75]. In all 12 cases, $X_0(N)$ is an elliptic curve over $\mathbb{Q}$ of rank 0, hence the number of non-cuspidal $\mathbb{Q}$-rational points is finite. For $N = 20, 24, 32, 36, 49$ there are no such points. For $N = 37$ the curve $X_0(N)$ has genus 2, for $N = 43$ it has

genus 3, for $N = 67$ it has genus 5 and for $N = 163$ it has genus 13. Every non-cuspidal $\mathbb{Q}$-rational point of an $X_0(N)$ corresponds to one specific j-invariant of an elliptic curve $E/\mathbb{Q}$. Out of the 26 values in the above theorem, the set

$$S := \{11, 14, 15, 17, 19, 21, 27, 37, 43, 67, 163\},$$

contains all 11 values of N, such that the genus of $X_0(N)$ is greater than 0. In Table 5.1 we present a complete list of all j-invariants corresponding to the non-cuspidal $\mathbb{Q}$-rational points on $X_0(N)$, for $N \in S$. For each j-invariant we give a global minimal model of an elliptic curve $E/\mathbb{Q}$ having this j-invariant. These models are taken from the Remarks on Isogenies and Table 1 in [lec75]. In each case, our given model is of lowest possible conductor and we state its Cremona label.

N	j-invariants	$E/\mathbb{Q}$	Label
11	$-11 \cdot 131^3$	$Y^2 + XY + Y = X^3 + X^2 - 30X - 76$	121a1
	-11^2	$Y^2 + XY + Y = X^3 + X^2 - 305X + 7888$	121a2
	-2^{15}	$Y^2 + Y = X^3 - X^2 - 7X + 10$	121b1
14	$-3^3 \cdot 5^3$	$Y^2 + XY = X^3 - X^2 - 2X - 1$	49a1
	$3^3 \cdot 5^3 \cdot 17^3$	$Y^2 + XY = X^3 - X^2 - 37X - 78$	49a2
15	$-5^2 \cdot 2^{-1}$	$Y^2 + XY + Y = X^3 - X - 2$	50a1
	$-5^2 \cdot 241^3 \cdot 2^{-3}$	$Y^2 + XY + Y = X^3 - 126X - 552$	50a2
	$-5 \cdot 29^3 \cdot 2^{-5}$	$Y^2 + XY + Y = X^3 - 76X + 298$	50a3
	$5 \cdot 211^3 \cdot 2^{-15}$	$Y^2 + XY + Y = X^3 + 549X - 2202$	50a4
17	$-17^2 \cdot 101^3 \cdot 2^{-1}$	$Y^2 + XY + Y = X^3 - 3041X + 64278$	14450p1
	$-17 \cdot 373^3 \cdot 2^{-17}$	$Y^2 + XY + Y = X^3 - 190891X - 36002922$	14450p2
19	$-2^{15} \cdot 3^3$	$Y^2 + Y = X^3 - 38X + 90$	361a1
21	$-3^2 \cdot 5^6 \cdot 2^{-3}$	$Y^2 + XY + Y = X^3 - X^2 - 5X + 5$	162b1
	$3^3 \cdot 5^3 \cdot 2^{-1}$	$Y^2 + XY + Y = X^3 - X^2 + 25X + 1$	162b2
	$-3^2 \cdot 5^3 \cdot 101^3 \cdot 2^{-21}$	$Y^2 + XY + Y = X^3 - X^2 - 95X - 697$	162b3
	$-3^3 \cdot 5^3 \cdot 383^3 \cdot 2^{-7}$	$Y^2 + XY + Y = X^3 - X^2 - 9695X - 364985$	162b4
27	$-2^{15} \cdot 3 \cdot 5^3$	$Y^2 + Y = X^3 - 30X + 63$	27a4
37	$-7 \cdot 11^3$	$Y^2 + XY + Y = X^3 - 201X + 1173$	1225g1
	$-7 \cdot 137^3 \cdot 2083^3$	$Y^2 + XY + Y = X^3 - 5202076X - 4567245077$	1225g2
43	$-2^{18} \cdot 3^3 \cdot 5^3$	$Y^2 + Y = X^3 - 860X + 9707$	1849a1
67	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	$Y^2 + Y = X^3 - 7370X + 243528$	4489a1
163	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	$Y^2 + Y = X^3 - 2174420X + 1234136692$	26569a1

Table 5.1.: All j-invariants corresponding to non-cuspidal rational points on $X_0(N)$, with $g(X_0(N)) > 0$.

Out of Mazur's and Kenku's result, one can immediately deduce that if an elliptic curve over $\mathbb{Q}$ possesses a cyclic isogeny of prime power degree, then this isogeny is

unique if the prime power is not 3 or 5 or a power of 2. The result is given in the next corollary and is used in the proof of the main Proposition 5.2.4 of the next section.

Corollary 5.1.12. *Let $N = \ell^e$ be a prime power of a prime $\ell \neq 2$ and let $E/\mathbb{Q}$ be an elliptic curve possessing a cyclic N-isogeny.*

(i) If $N \neq 3$ and $N \neq 5$, then this cyclic N-isogeny is unique.

(ii) If $N = 3$ or $N = 5$, then either this cyclic N-isogeny is unique or E has exactly two independent cyclic N-isogenies.

Proof. Consider all cyclic isogenies as a composition of cyclic isogenies of prime degree and look at the ℓ-isogeny graph of the elliptic curve $E/\mathbb{Q}$, i.e. the isogeny graph which contains exactly all isogenies of degree ℓ. The graph is constructed as follows. There is one vertex for each $\mathbb{Q}$-isomorphism class of elliptic curves $E'/\mathbb{Q}$, such that E and E' are isogenous by a composition of isogenies of degree ℓ. Then for each unordered pair of two vertices, choose an ordering of the corresponding elliptic curves, say E_1 and E_2. Then add an undirected edge between the two vertices for each isogeny $\eta : E_1 \to E_1$ of degree ℓ. The isogeny graph is independent of the chosen ordering, as each such isogeny $\eta : E_1 \to E_2$ of degree ℓ comes with a dual isogeny $\eta^\vee : E_2 \to E_1$ which is also of degree ℓ. Hence, each edge corresponds to the pair $(\eta, \eta^\vee)$. By construction, the ℓ-isogeny graph is connected and undirected, and it has never more than two edges per vertex, by Corollary 5.1.10. We claim that the graph has no cycles, i.e. the ℓ-isogeny graph is a linear graph.

To prove the claim, note that any path in the constructed graph which is not using twice the same edge defines a cyclic isogeny, and going back and forth the same edge gives the multiplication-by-ℓ endomorphism. Therefore, a cycle in the graph corresponds to an endomorphism of an elliptic curve which is cyclic, and thus is not a multiplication-by-n endomorphism, for some integer n. Hence, the existence of a cycle would give complex multiplication with the endomorphism defined over $\mathbb{Q}$, which is not possible. The claim follows.

By Mazur's and Kenku's classification 5.1.11 of cyclic isogenies, we get that the maximal number of edges in the linear ℓ-isogeny graph is equal to 1 if $\ell \geq 7$, equal to 2 if $\ell = 5$, and equal to 3 if $\ell = 3$. If $\ell \geq 7$, then all vertices correspond to elliptic curves possessing a unique cyclic ℓ-isogeny. If $\ell = 5$, then the two outer vertices correspond to elliptic curves possessing a unique cyclic 5^2-isogeny and a unique cyclic 5-isogeny, and the inner vertex corresponds to elliptic curves possessing independent cyclic 5-isogenies. If $\ell = 3$, then the two outer vertices correspond to elliptic curves possessing a unique cyclic 3^3-isogeny and a unique cyclic 3^2-isogeny and a unique cyclic 3-isogeny. The two inner vertices correspond to elliptic curves possessing a unique cyclic 3^2-isogeny and independent cyclic 3-isogenies. This completes the proof of the corollary. □

5.2. Cyclic isogenies $\Theta : E_1 \times E_2 \to B_\Theta$ with diagonal kernel, ($k = 13$)

In this section we loosen one of the assumptions we made in Setting 2.4.12. Instead of requiring that every point of the cyclic subgroup $G_i \subseteq E_i$ is $\mathbb{Q}$-rational, we merely demand that the G_i are Galois invariant. Hence, we consider arbitrary cyclic isogenies $\Theta : E_1 \times E_2 \to B_\Theta$ with diagonal kernel. Instead of working with the moduli space $X_1(N)$ we work with $X_0(N)$. By the end of this section, we show in Theorem 5.2.7 that if the order of $Ш(B_\Theta/\mathbb{Q})$ is finite and k denotes the non-square part of that order, then k equals one of the following eight values $\{1, 2, 3, 5, 6, 7, 10, 13\}$. Further, we present an example for the last missing case $k = 13$.

We are confronted with a new technical problem, namely how to determine whether G_1 and G_2 are isomorphic as Galois modules, i.e. how to determine whether two elliptic curves possess isogenies with isomorphic kernels. To solve this problem we use a theorem of Kraus and Oesterlé. It enables us to check for two elliptic curves over $\mathbb{Q}$, each with given cyclic isogeny of prime degree ℓ, whether the kernels of these isogenies are *not* isomorphic as Galois modules. Often it is also possible to use this method to verify that the kernels are isomorphic.

To state their theorem we introduce some notation. Denote by ℓ a prime number. Let E_1 and E_2 be two elliptic curves over $\mathbb{Q}$ with conductors N_1 and N_2. Denote by $\overline{\rho}_\ell(E_1)$ and $\overline{\rho}_\ell(E_2)$ their mod-ℓ Galois representations. Kraus and Oesterlé gave a computable criterion to check whether the semi-simplifications of $\overline{\rho}_\ell(E_1)$ and $\overline{\rho}_\ell(E_2)$ are isomorphic. For this purpose, they define an upper bound $\mu(E_1, E_2)$ in the following way. Let $S(E_1, E_2)$ be the product over all primes p, such that one of the two elliptic curves has split-multiplication reduction at p and the other one has non-split multiplicative reduction at p. Set

$$M(E_1, E_2) := S(E_1, E_2) \cdot \operatorname{lcm}(N_1, N_2), \text{ and}$$

$$\mu(E_1, E_2) := \frac{M(E_1, E_2)}{6} \cdot \prod_{p \mid M(E_1, E_2),\ p \text{ prime}} (1 + p^{-1}).$$

Theorem 5.2.1 (Kraus, Oesterlé). *Let E_1 and E_2 be elliptic curves over $\mathbb{Q}$ and let ℓ be a prime number. The following are equivalent:*

(i) The semi-simplifications of $\overline{\rho}_\ell(E_1)$ and $\overline{\rho}_\ell(E_2)$ are isomorphic.

(ii) For all primes p not dividing N_1N_2, we have $a_p(E_1) \equiv a_p(E_2) \bmod \ell$, and for all primes $p \mid N_1N_2$ such that $p^2 \nmid N_1N_2$, we have $a_p(E_1)a_p(E_2) \equiv p + 1 \bmod \ell$.

(iii) Same as (ii), but only for all primes $p < \mu(E_1, E_2)$.

Proof. This is Proposition 3 and 4 of [KO92]. □

Remark 5.2.2. Let E_1 and E_2 be elliptic curves over a number field K. If $E_1[\ell]$ and $E_2[\ell]$ are isomorphic as Galois modules, then the semi-simplifications of $\overline{\rho}_\ell(E_1)$ and $\overline{\rho}_\ell(E_2)$ are isomorphic. If both elliptic curves do not possess a cyclic ℓ-isogeny then the converse is also true. If both elliptic curves have cyclic ℓ-isogenies with isomorphic kernels

then the semi-simplifications of $\overline{\rho}_\ell(E_1)$ and $\overline{\rho}_\ell(E_2)$ are isomorphic. The converse is not true, but the next lemma shows that it is close to being true if $K = \mathbb{Q}$.

Lemma 5.2.3. *Let $\ell \neq 2$ be an odd prime number and let E_1 and E_2 be elliptic curves over $\mathbb{Q}$ having cyclic ℓ-isogenies $\theta_i : E_i \to E_i'$. Then the semi-simplifications of $\overline{\rho}_\ell(E_1)$ and $\overline{\rho}_\ell(E_2)$ are isomorphic if and only if either $\ker\theta_1 \cong \ker\theta_2$ or $\ker\theta_1 \cong \ker\theta_2^\vee$.*

Proof. Assuming that either $\ker\theta_1 \cong \ker\theta_2$ or $\ker\theta_1 \cong \ker\theta_2^\vee$, then it is clear that the semi-simplifications of $\overline{\rho}_\ell(E_1)$ and $\overline{\rho}_\ell(E_2)$ are also isomorphic. To prove the other direction, pick a basis of $E_i[\ell]$, such that the action of Galois is given by $\begin{pmatrix} a_i & * \\ 0 & d_i \end{pmatrix}$. By Corollary 5.1.10, there is a $\tau \in \mathrm{Gal}_\mathbb{Q}$, such that $a_i(\tau) \neq d_i(\tau)$, i.e. $\overline{\rho}_\ell(E_i)(\tau)$ has two different eigenvalues. Hence, the choice of basis for $E_i[\ell]$, such that the action of Galois is given by $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$, is unique up to multiples and ordering. Now assume that the semi-simplifications of $\overline{\rho}_\ell(E_1)$ and $\overline{\rho}_\ell(E_2)$ are isomorphic. It follows that either $a_1(\sigma)$ equals a multiple of $a_2(\sigma)$ or $a_1(\sigma)$ equals a multiple of $d_2(\sigma)$, for all $\sigma \in \mathrm{Gal}_\mathbb{Q}$. The former case is equivalent to $\ker\theta_1 \cong \ker\theta_2$ and the latter to $\ker\theta_1 \cong \ker\theta_2^\vee$. □

Recall, that the set of those N, such that $X_0(N)$ has at least one non-cuspidal rational point and is of genus larger than 0, is given by

$$S := \{11, 14, 15, 17, 19, 21, 27, 37, 43, 67, 163\}.$$

We present the main proposition of this section.

Proposition 5.2.4. *Let E_1 and E_2 be two elliptic curves over $\mathbb{Q}$ having cyclic N-isogenies with isomorphic kernels. If $N \in S$, then either E_1 and E_2 are isomorphic, or they are isogenous by a degree 2-isogeny. The latter case happens if and only if $N = 14$ and the j-invariants of E_1 and E_2 are different.*

Proof. As seen in Table 5.1, all occurring elliptic curves have j-invariant different from 0 or 1728, so we only have to consider quadratic twists by $[-1]$. We claim that the cyclic N-isogenies E_1 and E_2 possess are unique. For N being a prime power this is clear by Corollary 5.1.12. As the property of having a unique cyclic N-isogeny is stable under twisting by Lemma 5.1.5, it is sufficient to only check it for one representative of each remaining j-invariant. For $N = 14, 15, 21 = \ell_1 \cdot \ell_2$, with appropriate primes ℓ_i, one easily computes the factorisation of the ℓ_i-division polynomials for the given elliptic curves in Table 5.1 to deduce that the elliptic curves have unique cyclic ℓ_i-isogenies, and hence unique cyclic N-isogenies by Lemma 5.1.4.

As a direct consequence of the claim, we deduce by applying Lemma 5.1.5, that if E_1 and E_2 are non-isomorphic elliptic curves with cyclic N-isogenies with isomorphic kernels, then the j-invariants of the two elliptic curves have to be different. This settles the proposition for the cases $N = 19, 27, 43, 67, 163$ as there is only one j-invariant.

It remains to show that for a fixed $N \in \{11, 14, 15, 17, 21, 37\}$ there is no pair of elliptic curves having different j-invariants and cyclic N-isogenies with isomorphic kernels,

beside the case $N = 14$ in which the elliptic curves are isogenous by a degree 2-isogeny. For each pair of j-invariants, it is enough to fix one representative for one of the two j-invariants and then check whether there is a matching curve for the other j-invariant. This is due to Lemma 5.1.5.

To solve the case $N = 17$ or $N = 37$, we look at the factorisation of the kernel polynomials of the isogenies of the representatives given in Table 5.1. The kernel polynomials corresponding to $E('14450p1')$ and to $E('1225g2')$ are irreducible whereas the ones corresponding to $E('14450p2')$ and $E('1225g1')$ factor into two, respectively three, polynomials. By Lemma 5.1.6, if two elliptic curves have cyclic N-isogenies with isomorphic kernels, then the types of factorisation of the corresponding kernel polynomials are the same. Hence, there are no matching pairs with different j-invariant for $N = 17$ or 37.

To handle the cases $N = 15$ and $N = 21$, which both have four j-invariants each, we start by checking that there is a unique representative for each j-invariant having $\mathbb{Q}$-rational 3-torsion. These representatives are $E('50a1')$, $E('50a2')^{-3}$, $E('50a3')$, $E('50a4')^{-3}$ for $N = 15$, and $E('162b1')$, $E('162b2')^{-3}$, $E('162b3')$, $E('162b4')^{-3}$ for $N = 21$. Hence, it is sufficient to show that the 5-, respectively 7-, isogenies of these representatives have pairwise non-isomorphic kernels. This implies that only pairs of same j-invariant are possible, thus the curves have to be isomorphic.

To check that the 5-, respectively 7-, isogenies have pairwise non-isomorphic kernels, we are using two facts. Firstly, for a prime number ℓ, if two elliptic curves E_1 and E_2 have cyclic ℓ-isogenies with isomorphic kernels, then the semi-simplifications of their mod-ℓ Galois representations are isomorphic. Hence, by Theorem 5.2.1, $a_p(E_1) \equiv a_p(E_2) \mod \ell$, for all primes p, such that E_1 and E_2 have good reduction at p. For $N = 15$ the prime $p = 11$ is a prime of good reduction for all four representatives. Further, we have $a_{11}('50a1') = a_{11}('50a3') = -3$ and $a_{11}('50a2'^{-3}) = a_{11}('50a4'^{-3}) = 3$. Hence, we can exclude all but the two pairs $(E('50a1'), E('50a3'))$ and $(E('50a2')^{-3}, E('50a4')^{-3})$ from having 5-isogenies with isomorphic kernels. Secondly, the two elliptic curves in these exceptional pairs are isogenous by a 5-isogeny and they both possess a unique 5-isogeny. Hence, for them to have cyclic 5-isogenies with isomorphic kernels, the kernels of these isogenies have to be isomorphic to the kernels of the dual isogenies. But the kernel of a cyclic ℓ-isogeny with $\ell \neq 2$ cannot be isomorphic to the kernel of its dual isogeny by Corollary 5.1.10. This completes the case $N = 15$.

For $N = 21$ use the same strategy as for $N = 15$. The prime $p = 11$ again excludes all but the two pairs $(E('162b1'), E('162b3'))$ and $(E('162b2')^{-3}, E('162b4')^{-3})$. Proceed as for $N = 15$ to finish the case $N = 21$.

To show that pairs of elliptic curves with different j-invariants cannot have cyclic N-isogenies with isomorphic kernels for $N = 11$, we proceed as follows. Pick the three representatives $E('121a1')^{-11} = E('121c2')$, $E('121a2')$ and $E('121b1')$. We can assume all three elliptic curves to be given in short Weierstrass equations, say $Y^2 = f_{c2}(X)$, $Y^2 = f_{a2}(X)$ and $Y^2 = f_{b1}(X)$. The kernel polynomials of the 11-isogenies are in all three cases irreducible and have the same totally real splitting field L

of degree 5. Denote by x_{c2}, x_{a2}, respectively x_{b1}, a root of these kernel polynomials. Then the polynomials $Y^2 - f_{c2}(x_{c2})$, $Y^2 - f_{a2}(x_{a2})$, and $Y^2 - f_{b1}(x_{b1})$ factor in L into two linear factors, hence all three cyclic 11-isogenies have an L-kernel and this L is minimal. Using again Theorem 5.2.1 of Kraus and Oesterlé immediately shows that these three representatives do not have cyclic 11-isogenies with pairwise isomorphic kernels. As the degree of L is odd, it does not contain any quadratic subfield. By Lemma 5.1.2, twisting one of these elliptic curves with a quadratic extension $K = \mathbb{Q}(\sqrt{D})$ changes its 11-isogeny to be defined over $L(\sqrt{D})$, which is strictly bigger than L. Therefore, for every pair of elliptic curves of the given three representatives, if one fixes one member of this pair and runs over all twists of the other member, then one never obtains a pair of elliptic curves having 11-isogenies with isomorphic kernels. This finishes $N = 11$.

Now we come to the last case $N = 14$. There are two j-invariants and we claim that the representatives $E('49a1')$ and $E('49a2')$ have cyclic 14-isogenies with isomorphic kernels. Both elliptic curves have a rational 2-torsion point, hence it is sufficient to check that they have cyclic 7-isogenies with isomorphic kernels. One easily verifies that these two elliptic curves are isogenous by a degree 2-isogeny, hence they have isomorphic 7-torsion as Galois modules and thus the unique 7-isogenies they possess have isomorphic kernels. This completes the case for $N = 14$. □

Corollary 5.2.5. *Let E_1 and E_2 be elliptic curves over $\mathbb{Q}$ and let $\Theta : E_1 \times E_2 \to B_\Theta$ be a cyclic isogeny with diagonal kernel of degree N. If $N \in S$, then*

$$\#Ш(B_\Theta/\mathbb{Q}) = \square \quad or \quad \#Ш(B_\Theta/\mathbb{Q}) = 2 \cdot \square.$$

In particular, the case $\#Ш(B_\Theta/\mathbb{Q}) = 2 \cdot \square$ can only happen if $N = 14$ and the j-invariants of E_1 and E_2 are different.

Proof. Combine Corollary 2.4.16 with Proposition 5.2.4. □

It remains to study the case that $\Theta : E_1 \times E_2 \to B_\Theta$ is a cyclic isogeny with diagonal kernel whose degree N lies in the set

$$T := \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}.$$

A priori, we get the set $\{1, 2, 3, 5, 6, 7, 10, 13\}$ of square-free natural numbers k for the possible non-square parts of the order of some $Ш(B_\Theta/\mathbb{Q})$. In Chapter 3 we have already seen an example of all these cases but $k = 13$. The next examples shows that the value $k = 13$ also occurs as the non-square part of the order of Tate-Shafarevich groups of non-simple abelian surfaces $B_\Theta/\mathbb{Q}$.

Example 5.2.6. ($k = 13$) Consider the following two elliptic curves over $\mathbb{Q}$.

$$E_1 : Y^2 = X^3 - X^2 - 1829X - 32115,$$

$$E_2 : Y^2 = X^3 - X^2 - 1117108895940162813412069X$$
$$-4544555158992923683535961508147155 71.$$

The first curve has Cremona Label 2352j1, where $2352 = 2^4 \cdot 3 \cdot 7^2$. The second curve is of conductor $135694178256 = 2^4 \cdot 3 \cdot 7^2 \cdot 13 \cdot 251 \cdot 17681$. The two elliptic curves have cyclic 13-isogenies $\theta_i : E_i \to E_i'$ with isomorphic kernels, as their quadratic twists with respect to $D = 7$ have this property. This is due to Noam D. Elkies [Elk13]. One way of seeing this is to use Theorem 5.2.1 of Kraus and Oesterlé to show that the semi-simplifications of $\overline{\rho}_{13}(E_1)$ and $\overline{\rho}_{13}(E_2)$ are isomorphic (for the untwisted curves given by Elkies one has $S = 1$ and $\mu = 2201007876 + 2/3$). Together with Lemma 5.2.3, we deduce that either $\ker\theta_1 \cong \ker\theta_2$ or $\ker\theta_1 \cong \ker\theta_2^\vee$. Looking at the kernel polynomials of θ_1, θ_2, and $\theta_2^\vee$, we conclude that $\ker\theta_1 \cong \ker\theta_2$, as the kernel polynomials of θ_1 and θ_2 factor into two degree-3 factors, and the kernel polynomial of $\theta_2^\vee$ is irreducible. Thus $\ker\theta_1 \cong \ker\theta_2$ by Lemma 5.1.6.

Denote by $\Theta : E_1 \times E_2 \to B_\Theta$ the diagonal isogeny with respect to a Galois equivariant isomorphism $\alpha : \ker\theta_1 \to \ker\theta_2$. By Corollary 2.4.8, the order of $Ш(B_\Theta/\mathbb{Q})$ is independent of the choice of α. We prove that $\#Ш(B_\Theta/\mathbb{Q}) = 13 \cdot \square$.

As usual, we compute the global and the local quotient of the Cassels-Tate equation (2.1). It is not hard to check that the Mordell-Weil groups of all four elliptic curves E_1, E_2, E_1', and E_2' are trivial. Hence by Lemma 2.4.17, the global quotient equals 1 and we know that $Ш(B/\mathbb{Q})$ is finite, as the analytic ranks of the elliptic curves are all equal to 0. We claim that the local quotient at infinity also equals 1. As $2 \nmid \deg\Theta = 13$, we get that $\operatorname{coker}\Theta_\infty$ is trivial, by Lemma 2.2.23. To prove the claim it is sufficient to show that $\ker\theta_{1,\infty} = 0$. The kernel polynomial of θ_1 is

$$(X^3 - X^2 - 1829X + 6301)(X^3 + 195X^2 + 7187X + 71569).$$

Denote by $g_1(X)$ the first factor and by $g_2(X)$ the second factor of this kernel polynomial and by $f(X) := X^3 - X^2 - 1829X - 32115$ the defining polynomial of E_1. All six roots of g_1 and g_2 are real numbers and both factors g_1 and g_2 generate the same totally real Galois field of degree 3. Let x_0 be a zero of $g_1(X)$. As $y_0^2 = f(x_0) = g_1(x_0) - 38416 = 0 - 2^4 \cdot 7^4$, we get that $y_0 = \pm 2^2 \cdot 7^2 \cdot \sqrt{-1} \in \mathbb{C} \setminus \mathbb{R}$, which shows that $\ker\theta_{1,\infty}$ is trivial.

Among the four elliptic curves E_i and E_i', there are exactly two Tamagawa numbers which are divisible by 13. These are $c(E_2)_{13} = 13$ and $c(E_2')_{17681} = 13$. Note, that $c(E_2')_{13} = 1$ and $c(E_2)_{17681} = 1$. One easily verifies that $|\theta_i'(0)|_p = 1$, for all primes p and both i. Hence, by Corollary 2.2.22 we conclude that $\operatorname{coker}\theta_{1,p}$ is maximally unramified for all primes p and that $\operatorname{coker}\theta_{2,p}$ is maximally unramified for all $p \neq 13, 17681$.

Using Hensel's Lemma it follows that $g_1(X)$ and $g_2(X)$ both factor into linear factors in $\mathbb{Q}_{13}[X]$ and $\mathbb{Q}_{17681}[X]$. We conclude that $\ker\theta_{i,13}$ and $\ker\theta_{i,17681}$ both have 13 elements for both i, since $\sqrt{-1}$ also lies in $\mathbb{Q}_{13}$ and in $\mathbb{Q}_{17681}$. By Corollary 2.2.3, we get $H^1(\mathbb{Q}_{13}, E_i[\theta_i]) \cong H^1(\mathbb{Q}_{17681}, E_i[\theta_i]) \cong (\mathbb{Z}/13\mathbb{Z})^2$. Thus, $\operatorname{coker}\theta_{2,13}$ is trivial and $\operatorname{coker}\theta_{2,17681}$ is maximal, as $\#\operatorname{coker}\theta_{i,p}/\#\ker\theta_{i,p} = c(E_i')_p/c(E_i)_p$, by Corollary 2.2.14.

The Key Lemma 2.4.5 implies that the local quotient equals 1, for all $p \neq 13, 17681$, as in this case $\operatorname{coker}\Theta_p$ is maximally unramified. Further, the Key Lemma shows that $\operatorname{coker}\Theta_{13}$ is trivial and that $\operatorname{coker}\Theta_{17681}$ is maximally unramified. Hence, the local quotient for $p = 13$ equals $1/13$, and the local quotient for $p = 17681$ equals 1.

Putting everything together gives $\#Ш(B_\Theta/\mathbb{Q}) = 13 \cdot \#Ш(E_1 \times E_2/\mathbb{Q}) = 13 \cdot \square$.

The above example is probably not an example of an abelian surface having Tate-Shafarevich group of exact order 13, as the predicted size of the Tate-Shafarevich group of E_1 is 1 and of E_2 is 79^2. We summarise the results of this section, with the main contribution being Corollary 5.2.5, together with the examples provided in Chapter 3.

Theorem 5.2.7 (Classification of non-square parts of Tate-Shafarevich groups of abelian surfaces $B_\Theta/\mathbb{Q}$ being isogenous to a product of elliptic curves via a cyclic isogeny)**.** *Let $\mathcal{E}\ell\ell$ be the set of $\mathbb{Q}$-isomorphism classes of elliptic curves over $\mathbb{Q}$ having finite Tate-Shafarevich group. Then*

$$\{\#Ш(B_\Theta/\mathbb{Q}) \bmod \mathbb{Q}^{*2} \mid \exists \text{ a cyclic isogeny } \Theta : E_1 \times E_2 \to B_\Theta, \text{ and } E_1, E_2 \in \mathcal{E}\ell\ell\}$$

is a finite subset of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ and equals $\{1, 2, 3, 5, 6, 7, 10, 13\}$.

5.3. Diagonal multiplication-by-n maps $\Xi : E_1 \times E_2 \to B_\Xi$, ($k = 14$)

Let n be a positive integer and E_1 and E_2 be elliptic curves over a number field K. In this chapter, we study diagonal isogenies

$$\Xi : E_1 \times E_2 \to B_\Xi,$$

such that the kernel of Ξ is a diagonal embedding of the full n-torsion of the elliptic curves, i.e. there is a Galois equivariant isomorphism $\alpha : E_1[n] \to E_2[n]$ and the kernel of Ξ equals the graph of α. We call Ξ a *diagonal multiplication-by-n map*. In the style of Setting 2.4.12, we obtain the following associated diagram.

$$\begin{array}{ccccc} & & B_\Xi & & \\ & \overset{\Xi}{\nearrow} & & \overset{\psi}{\searrow} & \\ E_1 \times E_2 & & \xrightarrow{[n]_A = [n]_{E_1} \times [n]_{E_2}} & & E_1 \times E_2 \\ & \underset{\Xi^\vee}{\nwarrow} & & \underset{\psi^\vee}{\swarrow} & \\ & & B_\Xi^\vee & & \end{array} \tag{5.1}$$

The composition $\psi \circ \Xi$ as well as the dual map $\Xi^\vee \circ \psi^\vee$ are both the multiplication-by-n map on the product $E_1 \times E_2$. The kernels of all four maps $\Xi, \psi, \Xi^\vee, \psi^\vee$ and the full n-torsion of both elliptic curves are all pairwise isomorphic as Galois modules. The composition $\psi^\vee \circ \psi$ is a polarisation of B_Ξ of degree n^4.

Now we come back to find an answer to Question 1.2.4. If E_1 and E_2 are two isogenous elliptic curves over a number field K, then their ℓ-torsion points form isomorphic Galois modules for all but finitely many primes ℓ. Thus a priori, it seems possible to use diagonal multiplication-by-ℓ maps $\Xi : E_1 \times E_2 \to B_\Xi$ to get $Ш(B_\Xi/K) = \ell \cdot \square$, for arbitrary large ℓ, just by taking pairs of isogenous elliptic curves. But as seen in Proposition 2.4.10, if all Galois equivariant automorphism of $E_1[\ell]$ or $E_2[\ell]$ are

liftable to endomorphisms of E_1, respectively E_2, and ℓ does not divide the degree of an isogeny between E_1 and E_2, then B_Ξ is isomorphic to a product of two elliptic curves and hence the order of $\#Ш(B_\Xi/K)$ is a square. Additionally, the liftability condition implies that the order of $\#Ш(B_\Xi/K)$ is independent of the choice of the diagonal embedding of its kernel, by Proposition 2.4.7. Further, we can assume that E_1 and E_2 are isogenous by a cyclic isogeny, by Lemma 5.0.2. And finally, if a square-free positive integer k divides the degree of a cyclic isogeny between elliptic curves over $\mathbb{Q}$, then by Mazur's and Kenku's Theorem 5.1.11, k belongs to the finite set $\{1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 37, 43, 67, 163\}$. We summarise the discussion.

Corollary 5.3.1. *Consider the above situation of Diagram (5.1) and assume that all Galois equivariant automorphisms of $E_1[n]$ or $E_2[n]$ are induced by endomorphisms of E_1, respectively by endomorphisms of E_2. Then $\#Ш(B_\Xi/K)$ is independent of the choice of the isomorphism $\alpha : E_1[n] \to E_2[n]$. Assume additionally that E_1 and E_2 are isogenous by a cyclic isogeny of degree M and that $\#Ш(B_\Xi/K) = k \cdot \square$, with k square-free.*

(i) We have that $k \mid \gcd(M, n)$. In particular, if M is coprime to n, then B_Ξ is isomorphic to $E_1 \times E_2$ and $\#Ш(B_\Xi/K) = \square$.

(ii) If further $K = \mathbb{Q}$, then k equals one of the following 18 values: 1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 37, 43, 67, 163. In particular, the number of such possible k is finite.

Proof. The only implication which was not already contained in the above discussion is that k divides both n and M. This follows from Proposition 2.4.10, Remark 2.4.15, and the fact that elliptic curves have square order Tate-Shafarevich groups. □

It is still unknown to the author whether the order of $Ш(B_\Xi/\mathbb{Q})$ is always independent of the choice of α. We give a sufficient condition for the independence.

Proposition 5.3.2. *Let A be an abelian variety over a number field K. If the mod-n Galois representation $\overline{\rho}_n(A) : \mathrm{Gal}_K \to \mathrm{Aut}_{\overline{K}}(A[n])$ of A is surjective, then every Galois equivariant automorphism of $A[n]$ is multiplication by some $z \in (\mathbb{Z}/n\mathbb{Z})^*$. In particular, every Galois equivariant automorphism of $A[n]$ is induced by an endomorphism of A.*

Proof. Fix a basis of $A[n]$ to identify it with $(\mathbb{Z}/n\mathbb{Z})^{2d}$, for d being the dimension of A. Every automorphism β of $A[n]$ can be viewed as an element of $\mathrm{GL}_{2d}(\mathbb{Z}/n\mathbb{Z})$. As β is Galois equivariant it commutes with every element in the image of $\overline{\rho}_n(A)$, thus β lies in the center of $\mathrm{GL}_{2d}(\mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Aut}_{\overline{K}}(A[n])$. By the next lemma, β equals a multiple of the identity matrix and thus β is induced by a multiplication-by-z endomorphism of A, for some non-zero integer z, such that z is coprime to n. □

Next comes the missing lemma to finish the proof of Proposition 5.3.2. For a positive integer m, we denote with I_m the $(m \times m)$-identity matrix.

Lemma 5.3.3. *Let R be a commutative ring with unity and let m be a positive integer. Then the center of the general linear group $\mathrm{GL}_m(R)$ equals $\{z \cdot \mathrm{I}_m \mid z \in R^*\}$.*

Proof. This is an easy exercise and follows from the fact that $\mathrm{GL}_m(R)$ contains the elementary matrices which add the i-th row to the j-th row, if multiplied from the right, and the j-th column to the i-th column, if multiplied from the left. □

Remark 5.3.4. For non-CM elliptic curves the condition in the above Proposition 5.3.2 is almost always fulfilled. By Serre's Finite Image Theorem [Ser72], if E/K is a non-CM elliptic curve over a number field K, then the mod-ℓ^e Galois representation $\overline{\rho}_{\ell^e} : \mathrm{Gal}_K \to \mathrm{Aut}_{\overline{K}}(E[\ell^e])$ is surjective, for all but finitely many primes ℓ and all e. Note, that Serre's theorem is false for CM elliptic curves, as in this case $\overline{\rho}_\ell$ is not surjective for $\ell > 2$.

The following amazing theorem by Yuri Zarhin shows that one can actually do much better, as it is valid for arbitrary abelian varieties over arbitrary number fields.

Theorem 5.3.5 (Zarhin)**.** *Let A/K be an abelian variety over a number field K. Then there is a finite set $\mathbb{P}(A/K)$ of rational prime numbers, depending on A/K, such that for all prime powers ℓ^e, with $\ell \notin \mathbb{P}(A/K)$, every Galois equivariant endomorphism $\alpha : A[\ell^e] \to A[\ell^e]$ is induced by an endomorphism of A.*

Proof. This follows directly from Remark 5.4.7 in [Zar85]. □

Corollary 5.3.6 (Finitely many k for fixed pair of isogenous elliptic curves)**.** *Let E_1 and E_2 be isogenous elliptic curves over $\mathbb{Q}$ with finite Tate-Shafarevich groups. Then*

$$\{\#Ш(B/\mathbb{Q}) \bmod \mathbb{Q}^{*2} \mid \exists \text{ an isogeny } \varphi : E_1 \times E_2 \to B\}$$

is a finite subset of $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

Proof. We claim that there is a finite set $\tilde{\mathbb{P}}(E_1/\mathbb{Q}, E_2/\mathbb{Q})$ of rational prime numbers, such that if $\Xi : E_1 \times E_2 \to B_\Xi$ is a diagonal multiplication-by-n map, with n being a prime power ℓ^e, for a prime $\ell \notin \tilde{\mathbb{P}}(E_1/\mathbb{Q}, E_2/\mathbb{Q})$, then $\#Ш(B_\Xi/\mathbb{Q}) = \square$. Given the claim, the corollary follows from Remarks 2.4.3 and 2.4.15, Setting 5.0.3, and Theorem 5.2.7.

To prove the claim, we show that $\tilde{\mathbb{P}}(E_1/\mathbb{Q}, E_2/\mathbb{Q}) := \mathbb{P}(E_1/\mathbb{Q}) \cup \mathbb{P}(E_2/\mathbb{Q}) \cup \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$ has the property we want. The first two sets of the union are from Zarhin's Theorem 5.3.5 and the third one is the set of primes dividing the values given in Corollary 5.3.1(ii). The claim follows immediately. □

Now we consider the case of E_1 and E_2 being non-isogenous. We start with citing an important result of Faltings, for which we use the following notation. If A/K denotes an abelian variety over a number field K, then let $T_\ell(A)$ be the ℓ-adic Tate module, and denote by $L_v(A, s)$ the local L-series of A/K at a finite place $v \in M_K^0$.

Theorem 5.3.7 (Faltings)**.** *Let A and B be abelian varieties over a number field K. Then the following are equivalent:*

(i) A and B are isogenous,
(ii) $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong T_\ell(B) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ as Gal_K-modules, for all primes ℓ,
(iii) $L_v(A, s) = L_v(B, s)$ for almost all finite places $v \in M_K^0$,
(iv) $L_v(A, s) = L_v(B, s)$ for all finite places $v \in M_K^0$,

Proof. This is Corollary 2 in [Fal86]. □

Lemma 5.3.8. *Let E_1 and E_2 be non-isogenous elliptic curves over $\mathbb{Q}$. Then there is a finite set $\mathbb{P}(E_1/\mathbb{Q}, E_2/\mathbb{Q})$ of rational prime numbers, depending on $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$, such that for all prime powers ℓ^e, with $\ell \notin \mathbb{P}(E_1/\mathbb{Q}, E_2/\mathbb{Q})$, the Galois modules $E_1[\ell]$ and $E_2[\ell]$ are non-isomorphic.*

Proof. We proceed in two steps. Firstly, assume that there is a prime p, such that $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ have good reduction at p and $a_p(E_2) \neq a_p(E_2)$. By Theorem 5.2.1 of Kraus and Oesterlé, for all primes ℓ not dividing the difference $a_p(E_2) - a_p(E_2)$ the semi-simplifications of $\overline{\rho}_\ell(E_1)$ and $\overline{\rho}_\ell(E_2)$ are non-isomorphic. Thus, $E_1[\ell^e]$ and $E_2[\ell^e]$ can only be isomorphic as Galois modules if ℓ equals one of the finitely many primes dividing $a_p(E_2) - a_p(E_2)$.

Secondly, assume that for all primes p, such that $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ have good reduction at p, we have $a_p(E_2) = a_p(E_2)$. By definition of the local L-series at a place of good reduction, it follows that $L_p(E_1, s) = L_p(E_2, s)$, for all primes p, such that $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ have good reduction at p. In particular, the local L-series are equal for almost all p. Hence, by the above theorem of Faltings, we get that E_1 and E_2 are isogenous. □

Corollary 5.3.9 (Finitely many k for fixed pair of non-isogenous elliptic curves)**.** *Let E_1 and E_2 be non-isogenous elliptic curves over $\mathbb{Q}$ with finite Tate-Shafarevich groups. Then*

$$\{\#Ш(B/\mathbb{Q}) \bmod \mathbb{Q}^{*2} \mid \exists \text{ an isogeny } \varphi : E_1 \times E_2 \to B\}$$

is a finite subset of $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

Proof. The strategy is identical to the one applied in the proof of Corollary 5.3.6. Use $\tilde{\mathbb{P}}(E_1/\mathbb{Q}, E_2/\mathbb{Q}) := \mathbb{P}(E_1/\mathbb{Q}, E_2/\mathbb{Q})$ from the above Lemma 5.3.8. □

We deduce our best provable result possible to answer Question 1.2.4.

Corollary 5.3.10 (Finitely many k for finitely many elliptic curves)**.** *Let $\mathcal{E}\ell\ell^0$ be a finite set of $\mathbb{Q}$-isomorphism classes of elliptic curves over $\mathbb{Q}$ having finite Tate-Shafarevich groups. Then*

$$\{\#Ш(B/\mathbb{Q}) \bmod \mathbb{Q}^{*2} \mid \exists \text{ an isogeny } \varphi : E_1 \times E_2 \to B, \text{ and } E_1, E_2 \in \mathcal{E}\ell\ell^0\}$$

is a finite subset of $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

Proof. Follows immediately from Corollaries 5.3.6 and 5.3.9. □

We end our discussion about finding an answer to Question 1.2.4 by introducing two hypotheses, whose validity would result in a proof, that only finitely many square-free numbers k are possible for the non-square parts of the order of finite Tate-Shafarevich groups of non-simple abelian surfaces $B/\mathbb{Q}$. These two hypotheses claim that the finite sets $\mathbb{P}(E/\mathbb{Q})$ and $\mathbb{P}(E_1/\mathbb{Q}, E_2/\mathbb{Q})$ that occur in Corollaries 5.3.6 and 5.3.9 can be chosen independently of the elliptic curve(s).

Hypothesis 5.3.11. *There is a finite set $\mathbb{P}_1$ of prime numbers, such that if $E/\mathbb{Q}$ is an elliptic curve and ℓ^e is a prime power for a prime $\ell \notin \mathbb{P}_1$, then every Galois equivariant automorphism $\alpha : E[\ell^e] \to E[\ell^e]$ is induced by an endomorphism of E.*

Hypothesis 5.3.12. *There is a finite set $\mathbb{P}_2$ of prime numbers, such that if $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ are non-isogenous elliptic curves and ℓ^e is a prime power for a prime $\ell \notin \mathbb{P}_2$, then the Galois modules $E_1[\ell^e]$ and $E_2[\ell^e]$ are non-isomorphic.*

We deduce the conditional result that there are only finitely many square-free numbers that can occur as the order of the non-square part of $Ш(B_\Xi/\mathbb{Q})$, where $\Xi : E_1 \times E_2 \to B_\Xi$ is a diagonal multiplication-by-n map, for a suitable positive integer n.

Conditional Result 5.3.13 (Finitely many k for diagonal multiplication-by-n maps Ξ)**.** *Let $\mathcal{E}\ell\ell$ be the set of $\mathbb{Q}$-isomorphism classes of elliptic curves over $\mathbb{Q}$ having finite Tate-Shafarevich group. If the two Hypotheses 5.3.11 and 5.3.12 hold true, then*

$$\{\#Ш(B_\Xi/\mathbb{Q}) \bmod \mathbb{Q}^{*2} \mid \exists\, \Xi : E_1 \times E_2 \to B_\Xi, \text{ and } E_1, E_2 \in \mathcal{E}\ell\ell\}$$

is a finite subset of $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

Proof. Proceed as in the proofs of Corollaries 5.3.6 and 5.3.9. The finite set of primes $\mathbb{P}_1 \cup \mathbb{P}_2$ from the two Hypotheses 5.3.11 and 5.3.12 works for any pair of elliptic curves, whether they are isogenous or non-isogenous. □

Now we can give our conditional answer to Question 1.2.4 for non-simple abelian surfaces over the field of rational numbers.

Conditional Result 5.3.14 (Finitely many k for non-simple abelian surfaces $B/\mathbb{Q}$)**.** *Let $\mathcal{E}\ell\ell$ be the set of $\mathbb{Q}$-isomorphism classes of elliptic curves over $\mathbb{Q}$ having finite Tate-Shafarevich group. If the two Hypotheses 5.3.11 and 5.3.12 hold true, then*

$$\{\#Ш(B/\mathbb{Q}) \bmod \mathbb{Q}^{*2} \mid \exists \text{ an isogeny } \varphi : E_1 \times E_2 \to B, \text{ and } E_1, E_2 \in \mathcal{E}\ell\ell\}$$

is a finite subset of $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

Proof. As $B/\mathbb{Q}$ is non-simple, it is isogenous to a product of elliptic curves E_1 and E_2 via an isogeny having diagonal kernel, by Proposition 2.4.2. As already seen, the statement of this conditional result is equivalent to the conditional result given in 5.3.13. The equivalence follows from Setting 5.0.3 and the finiteness of the number of possible primes dividing the degrees of cyclic isogenies between elliptic curves over $\mathbb{Q}$, which is contained in Mazur's Theorem 5.1.11. □

Remark 5.3.15. A generalisation of the two hypotheses to abelian varieties of arbitrary dimension does not give the same conditional results about the finiteness of possible orders of non-square parts of Tate-Shafarevich groups of non-simple abelian varieties of some fixed dimension $d > 2$. This is due to the fact that isogenies between abelian varieties of dimension at least 2 do not always factor into a cyclic isogeny and a multiplication-by-n endomorphism. Hence, Setting 5.0.3 is more complicated in dimension $d > 2$. And a generalisation of the two hypotheses to elliptic curves over a fixed but arbitrary number field K is also not enough to get the conditional result

in 5.3.14 for elliptic curves over K, as one would also need a result similar to Mazur's Theorem 5.1.11 for elliptic curves over K.

We end this section by showing that there is a non-simple abelian surface $B/\mathbb{Q}$, such that $\#Ш(B/\mathbb{Q}) = 14 \cdot \square$, see Example 5.3.23. We achieve this result by combing a diagonal cyclic 7-isogeny and a diagonal multiplication-by-2 map. As usual, to determine the effect of diagonal multiplication-by-n maps $\Xi : E_1 \times E_2 \to B_\Xi$ on the order of Tate-Shafarevich groups, we want to calculate the quotient $\#Ш(E_1 \times E_2/K)/\#Ш(B_\Xi/K)$ obtained from the Cassels-Tate equation (2.1), which we divide into the global and the local quotient. By Remark 2.4.15, it is sufficient to study diagonal multiplication-by-n maps for $n = \ell^e$ being a primer power. We start with the local quotient at infinity.

Lemma 5.3.16. *Consider the above situation of Diagram (5.1) with $n = \ell^e$ being a prime power and let ∞ denote a place at infinity of K. If ∞ is a real place, assume further that either $\ell \neq 2$, or that $\ell = 2$ and the discriminants of the two elliptic curves E_1/K and E_2/K are negative. Then $\#\operatorname{coker}\Xi_\infty/\#\ker\Xi_\infty = 1/\ell^e$.*

Proof. If ∞ is a complex place, then the statement is trivial. A real place at infinity determines an embedding of K into $\mathbb{R}$, hence we can view E as an elliptic curve over $\mathbb{R}$. By [Sil94, V. Corollary 2.3.1], we have that $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ if and only if the discriminant of E/K is negative, and $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ otherwise. Hence, $\ker[\ell^e]_{1,\infty} \cong \ker[\ell^e]_{2,\infty} \cong \ker\Xi_\infty \cong \mathbb{Z}/\ell^e\mathbb{Z}$ and $\operatorname{coker}[\ell^e]_{1,\infty} = 0 = \operatorname{coker}[\ell^e]_{2,\infty}$. Therefore, $\operatorname{coker}\Xi_\infty$ is trivial by the Key Lemma 2.4.5. □

Now we have a look at the finite places for the usual multiplication-by-n endomorphism $[n]$ for abelian varieties A over number fields K.

Lemma 5.3.17. *Let A be an abelian variety over a number field K with a finite place v and let n be a positive integer. Consider the multiplication-by-n endomorphism $[n]$ of A. Then*

$$\#H^1(K_v, A[n]) = \#\ker[n]_v^2 \cdot p^{2\dim A \cdot v_p(n) \cdot [K_v:\mathbb{Q}_p]},$$

and

$$\frac{\#\operatorname{coker}[n]_v}{\#\ker[n]_v} = |[n]'(0)|_v^{-1} = p^{\dim A \cdot v_p(n) \cdot [K_v:\mathbb{Q}_p]}.$$

In particular, if $E/\mathbb{Q}$ is an elliptic curve and $n = \ell^e$ a prime power, then

$$\#H^1(\mathbb{Q}_p, E[\ell^e]) = \begin{cases} \#\ker[\ell^e]_p^2, & p \neq \ell \\ \#\ker[\ell^e]_p^2 \cdot \ell^{2e}, & p = \ell, \end{cases}$$

and

$$\frac{\#\operatorname{coker}[\ell^e]_p}{\#\ker[\ell^e]_p} = \begin{cases} 1 & , p \neq \ell, \\ \ell^e & , p = \ell. \end{cases}$$

Proof. The statement about the order of $H^1(K_v, A[n])$ follows directly from Lemma 2.2.1, as $A[n]^\vee = A[n]$, $\#A[n] = n^{2\dim A}$, and $\#H^0(K_v, A[n]) = \#\ker[n]_v$. The second state-

ment is Proposition 3.9 of [Sch96]. It is a direct corollary of Proposition 2.2.13 and the power series expansion of $[n]$ around the point at infinity. □

Using the results from Chapter 2, we obtain the following criterion for maximal unramifiedness of $\operatorname{coker}[\ell^e]_p$ for elliptic curves $E/\mathbb{Q}$.

Corollary 5.3.18. (Criterion for maximal unramifiedness of $\operatorname{coker}[\ell^e]_p$). *Let $E/\mathbb{Q}$ be an elliptic curve and denote by $[\ell^e] : E \to E$ the multiplication-by-ℓ^e map, for a prime power ℓ^e. Let $p \neq \ell$ be a prime, such that $\ell \nmid c_p$. Then $\operatorname{coker}[\ell^e]_p$ is maximally unramified.*

Proof. Follows directly from the above lemma and Corollary 2.2.20. □

We give an example of a diagonal multiplication-by-2 map $\Xi : E_1 \times E_2 \to B_\Xi$, such that $\#Ш(B_\Xi/\mathbb{Q}) = 2 \cdot \square$.

Example 5.3.19. Consider the following two elliptic curves over $\mathbb{Q}$

$$E_1 : Y^2 + XY + Y = X^3 + X^2 + 206340X - 407533347,$$

$$E_2 : Y^2 + XY + Y = X^3 + X^2 - 963294394250X + 508996941537511703.$$

Both elliptic curves do not possess a cyclic isogeny of degree 2. It follows from Theorem 5.2.1 of Kraus and Oesterlé that $E_1[2] \cong E_2[2]$ as Galois modules ($S = 13$ and $\mu = 131031820 + 5/6$). Let $[2]_i : E_i \to E_i$ denote the multiplication-by-2 endomorphism of E_i. Consider now the diagonal multiplication-by-2 map $\Xi : E_1 \times E_2 \to B_\Xi$. Using Sage, one can check that the mod-2 Galois representations of E_1 and E_2 are surjective. Therefore by Propositions 2.4.7 and 5.3.2, the order of $Ш(B_\Xi/\mathbb{Q})$ is independent of the choice of the Galois equivariant isomorphism $\alpha : E_1[2] \to E_2[2]$. We claim that this order is equal to $2 \cdot \square$.

The curves E_1 and E_2 are the quadratic twists by $D = 17$ of the two curves of Cremona label $'546f1'$ and $'98826t1'$. The conductor of E_1 is $2 \cdot 3 \cdot 7 \cdot 13 \cdot 17^2$ and the conductor of E_2 is $2 \cdot 3 \cdot 7 \cdot 13 \cdot 17^2 \cdot 181$, hence E_1 and E_2 are non-isogenous. Both elliptic curves have trivial Mordell-Weil group, hence by Lemma 2.4.17 the global quotient equals 1. Further, all Tate-Shafarevich groups are finite, as the analytic ranks equal 0. As both discriminants are negative, we get that the local quotient for the infinite place equals $1/2$, by Lemma 5.3.16.

The only Tamagawa number of both curves that is divisible by $\ell = 2$ is $c(E_2)_{181} = 2$ and the reduction type of E_2 at $p = 181$ is split multiplicative. Hence, for all finite primes $p \neq 2, 181$, we can apply Corollary 5.3.18 together with the Key Lemma 2.4.5 to deduce that $\operatorname{coker}\Xi_p$ is maximally unramified, and thus the local quotient for all finite primes $p \neq 2, 181$ is 1. We also know that $\operatorname{coker}[2]_{1,p=181}$ is maximally unramified.

The 2-division polynomial of E_1 has three solutions modulo 181. All three solutions are liftable via Hensel's Lemma to a 181-adic solution, hence $\ker[2]_{1,p=181}$, $\ker[2]_{2,p=181}$, and $\ker\Xi_{p=181}$ all have four elements each. By Lemma 5.3.17, $\operatorname{coker}[2]_{1,p=181}$ and $\operatorname{coker}[2]_{2,p=181}$ also have four elements each. As we already know that $\operatorname{coker}[2]_{1,p=181}$ equals the unramified subgroup, the question now is how much of $\operatorname{coker}[2]_{2,p=181}$ lies in $H^1_{\mathrm{nr}}(\mathbb{Q}_{181}, E_2[2])$. The answer is given in Lemma 5.3.20, stating that precisely two of

the four elements lie in $H^1_{\mathrm{nr}}(\mathbb{Q}_{181}, E_2[2])$. Hence by the Key Lemma 2.4.5, $\operatorname{coker}\Xi_{p=181}$ has two elements. As $\ker\Xi_{p=181}$ has four elements, the local quotient for $p = 181$ equals $1/2$. So far, the product of the global and local quotient equals $1/4$ and the only unknown datum is the local quotient for the prime $p = 2$.

The 2-division polynomial of E_1 factors into a linear and quadratic factor in $\mathbb{Q}_2[X]$, hence $\ker[2]_{1,p=2}$, $\ker[2]_{2,p=2}$, and $\ker\Xi_{p=2}$ have two elements. If $\xi : \mathrm{Gal}_{\mathbb{Q}_2} \to E_1[2]$ is a cocycle whose image lies in $\ker[2]_{1,p=2}$, then the image of the cocycle $\alpha^*(\xi)$ also lies in $\ker[2]_{2,p=2}$, for any given Galois equivariant isomorphism $\alpha : E_1[2] \to E_2[2]$. As the reduction type at $p = 2$ of both elliptic curves is split multiplicative, we can apply Lemma 5.3.21 to conclude that the isomorphism α^* induces an isomorphism between $\operatorname{coker}[2]_{1,p=2}$ and $\operatorname{coker}[2]_{2,p=2}$. Thus, by the Key Lemma 2.4.5, we deduce that the size of $\operatorname{coker}\Xi_2$ equals the size of $\operatorname{coker}[2]_{i,p=2}$. By Lemma 5.3.17, we have that $\operatorname{coker}[2]_{i,p=2}$ has four elements and hence the local quotient at $p = 2$ equals 2.

To sum up, we have $\#Ш(B_\Xi/\mathbb{Q}) = 2 \cdot \#Ш(E_1 \times E_2/\mathbb{Q}) = 2 \cdot \square$. The predicted size of the Tate-Shafarevich groups of the two elliptic curves by the Birch and Swinnerton-Dyer conjecture is 1, which would imply that $\#Ш(B_\Xi/\mathbb{Q}) = 2$.

We give the two lemmas which we need to compute the above example.

Lemma 5.3.20. *Let $E/\mathbb{Q}$ be an elliptic curve and denote by $[2] : E \to E$ the multiplication-by-2 map. Let $p \neq 2$ be a prime, such that E has split multiplicative reduction at p and that $E[2]$ is a trivial $\mathbb{Q}_p$-module, i.e. $\ker[2]_p$ has four elements. Then out of the four elements of $\operatorname{coker}[2]_p$ exactly two of them lie in $H^1_{\mathrm{nr}}(\mathbb{Q}_p, E[2])$.*

Proof. As the reduction type at p is multiplicative, there is an isomorphism $E(\mathbb{Q}_p) \cong \mathbb{Q}_p^*/q^{\mathbb{Z}}$, for some unique $q \in \mathbb{Q}_p^*$; see Theorem 2.3.2. Under this isomorphism $\ker[2]_p$ is identified with the set $\{\pm 1, \pm\sqrt{q}\}$, hence $\sqrt{q}$ also lies in $\mathbb{Q}_p^*$.

As $E[2]$ is a trivial $\mathbb{Q}_p$-module, we can identify $H^1_{\mathrm{nr}}(\mathbb{Q}_p, E[2])$ with the set of four homomorphism $\xi : \mathrm{Gal}(L/\mathbb{Q}_p) \to \{\pm 1, \pm\sqrt{q}\}$, where L is the unique unramified quadratic extension of $\mathbb{Q}_p$. We claim that exactly two of the homomorphisms ξ lie in the kernel of the natural map $\iota^1_{\mathrm{nr}} : H^1_{\mathrm{nr}}(\mathbb{Q}_p, E[2]) \to H^1(\mathbb{Q}_p, E(\overline{\mathbb{Q}}_p))$, i.e. the intersection of $H^1_{\mathrm{nr}}(\mathbb{Q}_p, E[2])$ with $\operatorname{coker}[2]_p$ consists of these two ξ's. Under this map ι^1_{nr}, ξ becomes trivial if and only if there is an element $P \in L^*$, such that $P^\tau/P = \xi(\tau)$, where τ denotes the non-trivial element of $\mathrm{Gal}(L/\mathbb{Q}_p)$. Note, that $P^\tau/P \in \mathbb{Q}_p^*$ if and only if P^τ/P equals ± 1 (this holds true for any quadratic field extension). Since $\xi(\tau) \in \mathbb{Q}_p^*$, we get that exactly the two ξ's corresponding to $\tau \mapsto \pm 1$ lie in the kernel of ι^1_{nr}. $\square$

Lemma 5.3.21. *Let $E/\mathbb{Q}$ be an elliptic curve and denote by $[2] : E \to E$ the multiplication-by-2 map. Assume E has split multiplicative reduction at $p = 2$ and that $\ker[2]_{p=2}$ has two elements. Then the four elements of $\operatorname{coker}[2]_{p=2}$ are represented in $H^1(\mathbb{Q}_2, E[2])$ precisely by those cocycles $\xi : \mathrm{Gal}_{\mathbb{Q}_2} \to E[2]$, such that the image of ξ lies in $\ker[2]_{p=2}$.*

Proof. Denote by W the quotient group $E[2]/\ker[2]_{p=2}$. Note, that W is a trivial $\mathbb{Q}_2$-Galois module. By Galois cohomology we get the exact sequence

$$0 \to W \to H^1(\mathbb{Q}_2, \ker[2]_{p=2}) \to H^1(\mathbb{Q}_2, E[2]).$$

Further, $H^1(\mathbb{Q}_2, \ker[2]_{p=2}) \cong (\mathbb{Z}/2\mathbb{Z})^3$, as there are precisely seven degree-2 extensions of $\mathbb{Q}_2$. Therefore, the image of $H^1(\mathbb{Q}_2, \ker[2]_{p=2})$ in $H^1(\mathbb{Q}_2, E[2])$ has order 4, as W has order 2. We claim that this image equals $\operatorname{coker}[2]_{p=2}$, which completes the proof. To see the claim, we have to show that

$$H^1(\mathbb{Q}_2, E[2]) \to H^1(\mathbb{Q}_2, E(\overline{\mathbb{Q}}_2))$$

is the zero map, when restricted to the image of $H^1(\mathbb{Q}_2, \ker[2]_{p=2})$ in $H^1(\mathbb{Q}_2, E[2])$. Pick a cocycle ξ representing a non-trivial element in $H^1(\mathbb{Q}_2, \ker[2]_{p=2})$, i.e. ξ is not a coboundary with respect to $\ker[2]_{p=2}$. We have to show that its image in $H^1(\mathbb{Q}_2, E(\overline{\mathbb{Q}}_2))$ is a coboundary. As the reduction type is split multiplicative we have an identification $E(\overline{\mathbb{Q}}_2) \cong \overline{\mathbb{Q}}_2^*/q^{\mathbb{Z}}$, for some $q \in \mathbb{Q}_2^*$; see Theorem 2.3.2. Under this isomorphism, $\ker[2]_{p=2}$ becomes identified with $\{\pm 1\}$. Thus ξ factors through a quadratic extension $L/\mathbb{Q}_2$, such that $\xi(\tau) = -1$, for τ being the non-trivial element in $\mathrm{Gal}(L/\mathbb{Q}_2)$. Choose a $P \in L$, such that $P^\tau = -P$. Such a P exists, because if one considers L as a two dimensional vector space over $\mathbb{Q}_2$, then it has a one-dimensional eigenspace for the eigenvalue -1. With respect to the map $\mathrm{Gal}_{\mathbb{Q}_2} \to \mathrm{Gal}(L/\mathbb{Q}_2)$, $\sigma \mapsto [\sigma]$, we get $P^\sigma/P = P^{[\sigma]}/P = \xi(\sigma)$, for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}_2}$. Thus, ξ becomes a coboundary in $H^1(\mathbb{Q}_2, E(\overline{\mathbb{Q}}_2))$, and the proof is complete. □

Now we look again at the two elliptic curves from Example 5.3.19 because they also possess cyclic isogenies of degree 7 with isomorphic kernels.

Example 5.3.22. Consider the following two elliptic curves over $\mathbb{Q}$ from Example 5.3.19

$$E_1 : Y^2 + XY + Y = X^3 + X^2 + 206340X - 407533347,$$

$$E_2 : Y^2 + XY + Y = X^3 + X^2 - 963294394250X + 508996941537511703.$$

They are the quadratic twists by $D = 17$ of the curves $E('546f1')$ and $E('98826t1')$, which both possess a rational 7-torsion point. Hence, E_1 and E_2 possess cyclic 7-isogenies with isomorphic kernels. Denote these cyclic isogenies by $\theta_i : E_i \to E_i'$ and fix a Galois equivariant isomorphism $\alpha : \ker\theta_1 \to \ker\theta_2$. Let $\Theta : E_1 \times E_2 \to B_\Theta$ be the cyclic isogeny with diagonal kernel, such that its kernel equals the graph of α. Recall from Corollary 2.4.8, that the order of $Ш(B_\Theta/\mathbb{Q})$ is independent from the choice of α. We claim that the order of $Ш(B_\Theta/\mathbb{Q})$ is equal to $7 \cdot \square$.

One easily checks that the Mordell-Weil groups of the four elliptic curves E_1, E_2, E_1' and E_2' are trivial, hence the global quotient for Θ is equal to 1, by Lemma 2.4.17. Further, all Tate-Shafarevich groups are finite, as the analytic ranks equal 0. By Lemma 5.1.2, $\ker\Theta$ has a $\mathbb{Q}(\sqrt{D})$-kernel, and as $D > 0$ we get that $\ker\Theta_\infty$ has seven elements. Since the degree of Θ is not divisible by 2, we get $\operatorname{coker}\Theta_\infty$ is trivial, by Lemma 2.2.23. Hence the local quotient at infinity equals $1/7$.

It is easy to check that $|\theta_i'(0)|_p = 1$ for all primes p and both i. For $p \neq 2, 13, 181$ all Tamagawa numbers are not divisible by 7, thus for all primes $p \neq 2, 7, 13, 181$ we have that $\operatorname{coker}\theta_{i,p}$ is maximally unramified for both i, due to Corollary 2.2.22. Therefore, the local quotient for $p \neq 2, 7, 13, 181$ equals 1, by the Key Lemma 2.4.5. By Corollary 2.2.14

we obtain $\#\operatorname{coker}\theta_{i,p}/\#\ker\theta_{i,p} = c(E_i')_p/c(E_i)_p$. As mentioned above, $\ker\theta_i$ has a $\mathbb{Q}_p$-kernel if and only if $\sqrt{D} \in \mathbb{Q}_p$, by Lemma 5.1.2. It follows that the kernel of $\theta_{i,p}$ is trivial for $p = 7, 181$ and has seven elements for $p = 2, 13$. We claim that for all four primes $p = 2, 7, 13, 181$ at least one of $\operatorname{coker}\theta_{1,p}$ and $\operatorname{coker}\theta_{2,p}$ is trivial, which by the Key Lemma 2.4.5 gives that $\operatorname{coker}\Theta_p$ is trivial for $p = 2, 7, 13, 181$.

For $p = 2$, the Tamagawa quotient $c(E_i')_p/c(E_i)_p$ equals $1/7$, for both i, hence $\operatorname{coker}\theta_{i,p=2}$ is trivial, for both i. For $p = 7$, the Tamagawa quotient equals 1 in both cases, giving a trivial cokernel for both i. For $p = 13$, the Tamagawa quotient for $i = 2$ equals $1/7$, hence $\operatorname{coker}\theta_{2,p=13}$ is trivial. For $p = 181$, the Tamagawa quotient for $i = 1$ equals 1, hence $\operatorname{coker}\theta_{1,p=181}$ is trivial. This completes the proof of the claim.

It follows that the local quotient for $p = 2, 13$ equals $1/7$, and for $p = 7, 181$ the local quotient equals 1. Hence, the local quotient equals $1/7^3$. We conclude that $\#Ш(B_\Theta/\mathbb{Q}) = 7^3 \cdot \#Ш(A/\mathbb{Q}) = 7 \cdot \square$. The predicted size of the Tate-Shafarevich groups of E_1 and E_2 is 1, hence we expect $\#Ш(B_\Theta/\mathbb{Q}) = 7^3$.

Combining the two above examples results in a non-simple abelian surface $B/\mathbb{Q}$, such that $\#Ш(B/\mathbb{Q}) = 14 \cdot \square$.

Example 5.3.23. ($k = 14$) Consider the following two elliptic curves over $\mathbb{Q}$ from Examples 5.3.19 and 5.3.22

$$E_1 : Y^2 + XY + Y = X^3 + X^2 + 206340X - 407533347,$$

$$E_2 : Y^2 + XY + Y = X^3 + X^2 - 963294394250X + 508996941537511703.$$

Let $G_i \subseteq E_i(\overline{\mathbb{Q}})$ be the set-theoretical union of the 2-torsion and the kernel of the degree-7 isogeny of E_i. Consider the diagonal isogeny $\varphi : E_1 \times E_2 \to B$ whose kernel equals the graph of a Galois equivariant isomorphism $\alpha : G_1 \to G_2$. Then the non-simple abelian surface $B/\mathbb{Q}$ has $\#Ш(B/\mathbb{Q}) = 14 \cdot \square$, independent of the choice of α.

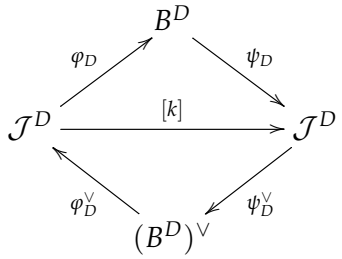
With notation from Setting 5.0.3, we obtain that $\#Ш(B_\Xi/\mathbb{Q}) = 2 \cdot \square$ and that $\#Ш(B_\Theta/\mathbb{Q}) = 7 \cdot \square$, independently of α. As the degree of the isogeny $B_\Xi \to B$ is coprime to 2, and the degree of the isogeny $B_\Theta \to B$ is coprime to 7, and the only primes dividing the degree of φ are 2 and 7, we get that $\#Ш(B/\mathbb{Q}) = 14 \cdot \square$.

Remark 5.3.24. For all primes ℓ up to 17, there are known examples of pairs of non-isogenous elliptic curves over $\mathbb{Q}$ having isomorphic ℓ-torsion, see [Fis11]. We would like to ask whether one can use such pairs to construct diagonal multiplication-by-ℓ maps $\Xi : E_1 \times E_2 \to B_\Xi$, such that $\#Ш(B/\mathbb{Q}) = \ell \cdot \square$, for $\ell \neq 2$. The corresponding moduli surface parametrising pairs of elliptic curves over $\mathbb{Q}$ having isomorphic ℓ-torsion is of general type for $\ell \geq 17$. It is an open problem for which primes $\ell > 17$ there are such pairs of non-isogenous elliptic curves. Finally, we would also like to ask, whether there is an abelian surface $A/\mathbb{Q}$ having non-square order Tate-Shafarevich group, such that $A/\mathbb{Q}$ is isogenous to two isogenous elliptic curves over $\mathbb{Q}$.

A Appendix A.

A brief glimpse at simple abelian surfaces, $(k = 11, 17, 23, 29)$

In the appendix, we briefly present a related but different technique to construct non-square order Tate-Shafarevich groups. Instead of considering isogenies possessed by a product of two elliptic curves over a number field K, one can also start with the Jacobian $\mathcal{J}$ of a smooth, projective curve C/K of genus g. If there is a K-rational torsion point $P \in \mathcal{J}(K)$ of exact order k, then dividing out the subgroup generated by P gives a cyclic isogeny $\varphi : \mathcal{J} \to B$ of degree k with K-kernel. As $\mathcal{J}$ is a principally polarised abelian variety over K of dimension g, the order of $Ш(\mathcal{J}/K)$ is a square or twice a square, if it is finite. Thus, we can use many results from Chapter 2 to compute the Cassels-Tate equation (2.1) with respect to $\varphi : \mathcal{J} \to B$. Let $\psi : B \to \mathcal{J}$ denote the isogeny of degree k^{2g-1}, such that $\varphi \circ \psi$ is the multiplication-by-k endomorphism of $\mathcal{J}$. Let D be a non-zero, square-free integer and consider the following twisted diagram.



(A.1)

If $K = \mathbb{Q}$, then the next proposition summarises sufficient conditions on k, D, $\mathcal{J}$ and $\mathcal{J}^D$ to guarantee that $\#Ш(B^D/\mathbb{Q}) = k \cdot \square$, provided it is finite. If $C/\mathbb{Q}$ is a hyperelliptic curve, then in principle it is possible to check the given conditions using Magma.

Proposition A.1. *With notation as above, assume that*

(i) $D > 0$, *k square-free, and* $\gcd(2D, k) = 1$,

(ii) the Mordell-Weil rank of $\mathcal{J}^D$ *equals* 0,

(iii) the order of $Ш(\mathcal{J}^D/\mathbb{Q})$ *is a square, if it is finite,*

(iv) $\mathcal{J}$ *and* $\mathcal{J}^D$ *have good reduction at all primes* $\ell \mid k$,

(v) there are finitely many primes $p_1, \dots, p_m$ *all unequal to* 2, *such that* $\mathcal{J}^D$ *has good reduction at all* p_j *and* $\gcd(k, \#\mathcal{J}^D(\mathbb{F}_{p_1}), \dots, \#\mathcal{J}^D(\mathbb{F}_{p_m})) = 1$,

(vi) for all primes p *such that* $\mathcal{J}^D$ *has bad reduction at* p, *we have* $\sqrt{D} \notin \mathbb{Q}_p$,

(vii) for all primes p *such that* $\mathcal{J}^D$ *has bad reduction at* p *and for all primes* $\ell \mid k$, *we have* $\mathbb{Q}_p(\sqrt{D}) \neq \mathbb{Q}_p(\boldsymbol{\mu}_\ell)$.

Then $\#Ш(B^D/\mathbb{Q}) = k \cdot \square$, *if the order is finite.*

Proof. As usual, we compute the global and local quotient of the Cassels-Tate equation with respect to the isogeny $\varphi_D : \mathcal{J}^D \to B^D$. Since the Mordell-Weil rank of $\mathcal{J}^D$ equals 0 we get that the regulator quotient equals 1. Now let $p_1, \dots, p_m$ be as in assumption (v). Combining Lemmas 2.2.6 and 2.2.17 yields that $\gcd(k, \#\mathcal{J}^D(\mathbb{Q})_{\text{tors}}) = \gcd(k, \#B^D(\mathbb{Q})_{\text{tors}}) = \gcd(k, \#(B^D)^\vee(\mathbb{Q})_{\text{tors}}) = 1$. This implies that neither one of the four isogenies $\varphi_D, \varphi_D^\vee, \psi_D, \psi_D^\vee$ has a non-trivial $\mathbb{Q}$-rational point in its kernel. It follows that the torsion quotient equals 1, by an argument similar to the one used in the proof of Lemma 2.4.17. Therefore, the global quotient equals 1.

As D is positive and $2 \nmid k$, use Lemmas 2.2.23 and 5.1.2 to get that the local quotient at infinity equals $1/k$, as the cokernel is trivial and the kernel is defined over the reals. Now we show that the local quotient for all finite primes equals 1, which completes the proof, since $\#Ш(\mathcal{J}^D/\mathbb{Q})$ is assumed to be a square, if it is finite.

By Corollary 2.2.11, if $p \nmid k$ is a place of good reduction, then the local quotient for p is 1. Now let ℓ be a prime dividing k. Then it is a prime of good reduction for $\mathcal{J}$ and $\mathcal{J}^D$ by assumption (iv). As φ has a $\mathbb{Q}_\ell$-kernel it follows with Corollary 2.2.22 that $|\varphi'(0)|_\ell = 1$. Hence, by Lemma 5.1.3 we get that $|\varphi'_D(0)|_\ell = 1$, as $\ell \nmid D$ by assumption (i). Using again Corollary 2.2.22 implies that the local quotient for ℓ equals 1, as the cokernel of φ_D is maximally unramified over $\mathbb{Q}_\ell$.

Now we consider the primes of bad reduction. Let ℓ be a prime dividing k and recall the notation $\varphi_{D,\ell}$ and $\varphi_{D,\ell}^\vee$ from Remark 2.4.15. We claim that for all $\ell \mid k$ neither $\varphi_{D,\ell}$ nor $\varphi_{D,\ell}^\vee$ has a $\mathbb{Q}_p$-kernel, for p a prime of bad reduction for $\mathcal{J}^D$. As k is square-free we deduce from Corollary 2.2.2 that the local quotient of $\varphi_{D,\ell}$ at p equals 1, which gives that the local quotient of φ_D at p is 1, for all primes p of bad reduction.

It remains to prove the claim. From assumption (vi) and Lemma 5.1.2 it follows that $\varphi_{D,\ell}$ has a $\mathbb{Q}_p(\sqrt{D})$-kernel and not a $\mathbb{Q}_p$-kernel, as $\ell \neq 2$. Now assume to the contrary that $\varphi_{D,\ell}^\vee$ has a $\mathbb{Q}_p$-kernel. Due to Cartier duality this would imply that $\varphi_{D,\ell}$ has a $\mathbb{Q}_p(\boldsymbol{\mu}_\ell)$-kernel and does not have a L-kernel, for each proper subfield $L \subsetneq \mathbb{Q}_p(\boldsymbol{\mu}_\ell)$. As $\varphi_{D,\ell}$ has a $\mathbb{Q}_p(\sqrt{D})$-kernel and not a $\mathbb{Q}_p$-kernel and $[\mathbb{Q}_p(\sqrt{D}) : \mathbb{Q}_p] = 2$, we get a contradiction by assumption (vii). $\square$

Remark A.2. For each prime $\ell \neq 2$, the equation $Y^2 + Y = X^\ell$ determines a hyperelliptic curve $C/\mathbb{Q}$ of genus $(\ell-1)/2$, such that $\mathcal{J}(\mathbb{Q})$ contains a point of exact order ℓ. This follows from the fact that the divisor of Y is $\ell((0,0)) - \ell(\infty)$ and was communicated to me by Tim Dokchitser. Thus, it seems very likely that Proposition A.1 enables one to find an abelian variety $B/\mathbb{Q}$ of dimension $(\ell-1)/2$, such that $\#Ш(B/\mathbb{Q}) = \ell \cdot \square$, for any given prime $\ell \geq 5$, provided the order of $Ш(B/\mathbb{Q})$ is finite. This supports William Stein's Conjecture 1.2.3. Nevertheless, it is unknown which values of k are possible for a fixed genus g and fixed number field K. Even for $g = 2$ and $K = \mathbb{Q}$ this is an unsolved problem.

Now we give four examples of hyperelliptic curves $C/\mathbb{Q}$, such that their Jacobians $\mathcal{J}$ possess a $\mathbb{Q}$-rational point of order $k = 11$, 17, 23 and 29, respectively. The curve with $k = 17$ is from Elkies [Elk02], and the other three are from Leprévost [Lep95]. Using a result of [Lep95], Elkies and Leprévost proved in all four cases that the Jacobians $\mathcal{J}$ are absolutely simple over $\mathbb{Q}$, i.e. they are simple over $\overline{\mathbb{Q}}$. In particular, every quadratic twist $\mathcal{J}^D$ and every abelian variety being isogenous to $\mathcal{J}^D$ are simple over $\mathbb{Q}$. In the remaining of the appendix, we use the above Proposition A.1 to find a suitable twist J^D of each of the Jacobians of the four given curves, such that $Ш(B^D/\mathbb{Q})$ has order k times a square, provided it is finite. If $C : Y^2 = f(X)$ is a hyperelliptic curve with Jacobian $\mathcal{J}$, then for a square-free non-zero integer D the twisted Jacobian $\mathcal{J}^D$ equals the Jacobian of the twisted curve $C^D : Y^2 = D \cdot f(X)$.

Example A.3. ($k = 17$) Consider the following hyperelliptic curve of genus 2 over $\mathbb{Q}$.

$$C : Y^2 = (9X^2 + 2X + 1)(32X^3 + 81X^2 - 6X + 1)$$

By [Elk02], its Jacobian $\mathcal{J}$ has a $\mathbb{Q}$-rational torsion point of order $k = 17$. We claim that for $D = 3$, the order of the Tate-Shafarevich group of the abelian surface $B^D/\mathbb{Q}$ is equal to $17 \cdot \square$, assuming it is finite.

We check the seven conditions of Proposition A.1. Assumption (i) is obvious and (ii) and (iii) can be checked with Magma. Further, Magma tells us that $\mathcal{J}^D$ has good reduction outside of $2, 3, 31$, and $\mathcal{J}$ has good reduction outside of $2, 31$, giving (iv). For $p = 5$ one can use Magma to compute $\#\mathcal{J}^D(\mathbb{F}_5) = 22$ to get (v). To check (vi) and (vii), one can use Sage or an algorithm of John W. Jones and David P. Roberts [JR11].

Remark A.4. We expect that there are infinitely many $D > 0$ such that in the above example the conditions of Proposition A.1 are fulfilled. Probably most positive primes D being a quadratic non-residue modulo $3, 17, 31$ and not being congruent 1 mod 8, such that $\mathcal{J}^D$ has rank equal to 0 and a quadratic Tate-Shafarevich group fulfill the conditions. For example, the twists of $D = 827$ and 947 have non-square order Ш.

We give our final three examples, completing the proof of Theorem 1.2.5.

Example A.5. ($k = 11, 23, 29$) Consider the following hyperelliptic curve of genus 2 over $\mathbb{Q}$.

$$C_{11} : Y^2 = (2X^2 - 2X + 1)(2X^4 - 2X^3 + X^2 - 4X + 4)$$

A. Appendix. A brief glimpse at simple abelian surfaces, $(k = 11, 17, 23, 29)$

$$C_{23} : Y^2 = X^6 - 10X^5 + 33X^4 - 36X^3 + 28X^2 - 16X + 4$$
$$C_{29} : Y^2 = (2X - 1)(2X^5 - X^4 - 4X^2 + 8X - 4)$$

By [Lep95], the Jacobian $\mathcal{J}$ of C_k has a $\mathbb{Q}$-rational torsion point of order k. Choosing $D = 3$, $D = 3$, and $D = 2$, respectively, and assuming that the Tate-Shafarevich group of the abelian surface $B^D/\mathbb{Q}$ is finite, then it follows from Proposition A.1 that the order of $Ш(B^D/\mathbb{Q})$ equals $11 \cdot \square$, respectively $23 \cdot \square$, respectively $29 \cdot \square$.

Bibliography

[Art86] M. Artin. Néron models. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 213–230. Springer, New York, 1986.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993), `http://magma.maths.usyd.edu.au/magma/`.

[Cas62] J. W. S. Cassels. Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. *J. Reine Angew. Math.*, 211:95–112, 1962.

[Cas65] J. W. S. Cassels. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 217:180–199, 1965.

[Dal10] Chandan Singh Dalawat. Local discriminants, Kummerian extensions, and elliptic curves. *J. Ramanujan Math. Soc.*, 25(1):25–80, 2010.

[DD13] Tim Dokchitser and Vladimir Dokchitser. Local invariants of isogenous elliptic curves, 2013. Preprint, `http://arxiv.org/abs/1208.5519v3`.

[Dok05] Vladimir Dokchitser. Root numbers of non-abelian twists of elliptic curves. *Proc. London Math. Soc. (3)*, 91(2):300–324, 2005. With an appendix by Tom Fisher.

[Elk02] Noam D. Elkies. Curves of genus 2 over Q whose Jacobians are absolutely simple abelian surfaces with torsion points of high order, 2002. Published online on the authors webpage, `http://www.math.harvard.edu/~elkies/g2_tors.html`.

[Elk13] Noam D. Elkies. Elliptic curves over QQ with identical 13-isogeny, 2013. Published online as an answer on mathoverflow.net, `http://mathoverflow.net/questions/129818/elliptic-curves-over-qq-with-identical-13-isogeny`.

[Fal86] Gerd Faltings. Finiteness theorems for abelian varieties over number fields. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 9–27. Springer, New York, 1986. Translated from the German original [Invent. Math. 73 (1983), no. 3, 349–366; ibid. 75 (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz.

[FG08] E. V. Flynn and C. Grattoni. Descent via isogeny on elliptic curves with large rational torsion subgroups. *J. Symbolic Comput.*, 43(4):293–303, 2008.

[Fis00] Thomas Anthony Fisher. *On 5 and 7 Descents for Elliptic Curves*. PhD thesis, Clare College, 2000. `https://www.dpmms.cam.ac.uk/~taf1000/thesis.html`.

[Fis01] Tom Fisher. Some examples of 5 and 7 descent for elliptic curves over $\mathbf{Q}$. *J. Eur. Math. Soc. (JEMS)*, 3(2):169–201, 2001.

[Fis11] Tom Fisher. On families of n-congruent elliptic curves. `https://www.dpmms.cam.ac.uk/~taf1000/papers/highercongr.html`, 2011.

[Fla90] Matthias Flach. A generalisation of the Cassels-Tate pairing. *J. Reine Angew. Math.*, 412:113–127, 1990.

[Hil95] Gregory Hill. Regular elements and regular characters of $\mathrm{GL}_n(\mathcal{O})$. *J. Algebra*, 174(2):610–635, 1995.

[HLP98] Everett W. Howe, Franck Leprévost, and Bjorn Poonen. Large Torsion Subgroups Of Split Jacobians Of Curves Of Genus Two Or Three. *FORUM MATH*, 12:315–364, 1998.

[Jor05] Andrei Jorza. The Birch and Swinnerton-Dyer Conjecture for Abelian Varieties over Number Fields. Master's thesis, Harvard University, 2005. `http://www3.nd.edu/~ajorza/`.

[JR11] John W. Jones and David P. Roberts. Database of Local Fields. `http://math.la.asu.edu/~jj/localfields/`, 2011.

[Kat81] Nicholas M. Katz. Galois properties of torsion points on abelian varieties. *Invent. Math.*, 62(3):481–502, 1981.

[Kei12] Stefan Keil. Sage Worksheet: On the density of non-square order Tate-Shafarevich groups. `http://www.sagenb.org/home/pub/4330/`, 2012.

[Kei13] Stefan Keil. Examples of non-simple abelian surfaces over the rationals with non-square order Tate-Shafarevich group. Preprint, `http://arxiv.org/abs/1206.1822/`, 2013.

[Ken82] M. A. Kenku. On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class. *J. Number Theory*, 15(2):199–202, 1982.

[KK13] Stefan Keil and Remke N. Kloosterman. On the density of abelian surfaces with Tate-Shafarevich group of order five times a square. In *ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium, San Diego 2012*, volume 1 of *Open Book Series*, pages 413–435. Mathematical Sciences Publishers, Berkeley, 2013.

[Klo01] Remke Kloosterman. Elliptic curves with large Selmer groups. `http://www.mathematik.hu-berlin.de/~klooster/publ.php`, 2001.

[Klo05] Remke Kloosterman. The p-part of the Tate-Shafarevich groups of elliptic curves can be arbitrarily large. *J. Théor. Nombres Bordeaux*, 17(3):787–800, 2005.

[KO92] A. Kraus and J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293(2):259–275, 1992.

[KS99] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1999.

[KS03] Remke Kloosterman and Edward F. Schaefer. Selmer groups of elliptic curves that can be arbitrarily large. *J. Number Theory*, 99(1):148–163, 2003.

[Lan56] Serge Lang. Algebraic groups over finite fields. *Amer. J. Math.*, 78:555–563, 1956.

[lec75] In W. Kuyk and B. J. Birch, editors, *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975.

[Lep95] Franck Leprévost. Jacobiennes de certaines courbes de genre 2: torsion et simplicité. *J. Théor. Nombres Bordeaux*, 7(1):283–306, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[Lig75] Gérard Ligozat. *Courbes modulaires de genre* 1. Société Mathématique de France, Paris, 1975. Bull. Soc. Math. France, Mém. 43, Supplément au Bull. Soc. Math. France Tome 103, no. 3.

[Mat55] Arthur Mattuck. Abelian varieties over p-adic ground fields. *Ann. of Math. (2)*, 62:92–119, 1955.

[Mat07] Kazuo Matsuno. Construction of elliptic curves with large Iwasawa λ-invariants and large Tate-Shafarevich groups. *Manuscripta Math.*, 122(3):289–304, 2007.

[Maz77a] B. Mazur. Rational points on modular curves. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 107–148. Lecture Notes in Math., Vol. 601. Springer, Berlin, 1977.

[Maz77b] Barry Mazur. Modular curves and the Eisenstein ideal. *IHES Publ. Math.*, 47:33–186, 1977.

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Mil72] J. S. Milne. On the arithmetic of abelian varieties. *Invent. Math.*, 17:177–190, 1972.

[Mil06] J.S. Milne. *Arithmetic Duality Theorems*. BookSurge, LLC, second edition, 2006.

[Mil08] J.S Milne. Abelian varieties 2.0. `http://www.jmilne.org/math/CourseNotes/`, 2008.

[Mor23] L. J. Mordell. On the Rational Solutions of the Indeterminate Equations of Third and Fourth degrees. *Proc. of the Cambridge Phil. Society*, **21**:179–192, 1923.

[Par05] Pierre J. R. Parent. Towards the triviality of $X_0^+(p^r)(\mathbf{Q})$ for $r > 1$. *Composition Math.*, 141:561–572, 2005.

[PS99] Bjorn Poonen and Michael Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)*, 150(3):1109–1149, 1999.

[S$^+$13] William A. Stein et al. Sage, open-source mathematics software system licensed under the GPL, version 4.6.2. `http://www.sagemath.org/`, 2013.

[Sch96] Edward F. Schaefer. Class groups and Selmer groups. *J. Number Theory*, 56(1):79–114, 1996.

[Sch98] Edward F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.*, 310(3):447–471, 1998.

[SD67] P. Swinnerton-Dyer. The conjectures of Birch and Swinnerton-Dyer, and of Tate. In *Proc. Conf. Local Fields (Driebergen, 1966)*, pages 132–157. Springer, Berlin, 1967.

[Ser72] Jean-Pierre Serre. Properties galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15:259–331, 1972.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, English edition, 2002.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[SS01] Edward F. Schaefer and Michael Stoll. How to do a p-descent on an elliptic curve. long online version, 2001.

[SS04] Edward F. Schaefer and Michael Stoll. How to do a p-descent on an elliptic curve. *Trans. Amer. Math. Soc.*, 356(3):1209–1231 (electronic), 2004.

[Ste03] William A. Stein. Possibilities for Shafarevich-Tate Groups of Modular Abelian Varieties, March 2003. `http://modular.math.washington.edu/papers/nonsquaresha/`.

[Ste04] William A. Stein. Shafarevich-Tate groups of nonsquare order. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 277–289. Birkhäuser, Basel, 2004.

[Ste09] William A. Stein. Computational verfication of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves. *Math. Comp.*, 78:2397–2425, 2009.

[Tat63] John Tate. Duality theorems in Galois cohomology over number fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 288–295. Inst. Mittag-Leffler, Djursholm, 1963.

[Tat75] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975.

[Tat95] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages 415–440. Soc. Math. France, Paris, 1995.

[vdGM11] Gerard van der Geer and Ben Moonen. *Abelian Varieties*. 2011. Preliminary version, `http://staff.science.uva.nl/~bmoonen/boek/BookAV.html`.

[Vél71] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[Wei29] André Weil. L'arithmétique sur les courbes algébriques. *Acta Math.*, 52(1):281–315, 1929.

[Zar85] Yu. G. Zarhin. A finiteness theorem for unpolarized abelian varieties over number fields with prescribed places of bad reduction. *Invent. Math.*, 79(2):309–321, 1985.

Selbständigkeitserklärung

Hiermit erkläre ich, daß ich die vorliegende Arbeit selbständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Berlin, den 29.11.2013 Stefan Keil